Guide de l'utilisateur

Linksys E1550 | Routeur sans fil N avec SpeedBoost[MC]

Table des matières

Présentation du produit

Contenu de la boîte 4
Fonctionnalités 4
Vue arrière 5
Vue de dessous 6

Configuration : Opérations de base

Création d'un réseau domestique 7
Qu'est-ce qu'un réseau? 7
Installation d'un réseau domestique 7
Pour obtenir de l'aide 7
Configuration de votre routeur 7
Lancement de Cisco Connect 8
Installation de Cisco Connect sur un autre ordinateur 9
Amélioration de la vitesse de votre connexion sans fil 9
Test de la vitesse de votre connexion sans fil 9
Connexion de périphériques à votre réseau 10
Connexion d'un ordinateur à votre réseau 10
Connexion d'une imprimante 12
Connexion d'autres périphériques 13
Configuration du contrôle parental 14
Accès au contrôle parental 14
Choix des ordinateurs soumis au contrôle parental 15
Paramétrage du contrôle parental 16
Configuration d'un accès d'invité 16
Modification du nom et du mot de passe du routeur 17

Configuration : Avancée

Ouverture de l'utilitaire Web 18
Configuration manuelle de votre routeur 18
Configuration manuelle de votre connexion Internet 19
Configuration du serveur DHCP sur votre routeur 20
Configuration de la réservation DHCP 20
Localisation de votre réseau sur Internet 21
Clonage d'adresse MAC 22
Connexion au réseau de votre bureau à l'aide d'un VPN 22
Optimisation de votre routeur pour les jeux et les communications vocales 23
Modification à distance des paramètres du routeur 24
Activation de la voix sur IP sur votre réseau 25
Configuration de la fonction UPnP 26
Utilisation d'un routeur en tant que point d'accès 26
Installation de votre nouveau routeur derrière l'ancien 28
Ajout de votre routeur à un routeur ou une passerelle 28
Partage d'une connexion Internet 29
Extension de votre réseau 30
Exposition d'un périphérique sur Internet 31

Optimisation de la sécurité

Comment savoir si mon réseau est sécurisé? 33
Sécurité du réseau après une configuration manuelle 33
Configuration de la sécurité sans fil à l'aide de la fonction Wi-Fi Protected Setup 34
Voyant d'activité Wi-Fi Protected Setup 34

Connexion d'un périphérique à l'aide du bouton Wi-Fi Protected Setup 34
Connexion d'un périphérique à l'aide de son NIP Wi-Fi Protected Setup 35
Connexion d'un périphérique à l'aide du NIP Wi-Fi Protected Setup du routeur 35
Connexion manuelle d'un périphérique 35
Contrôle de l'accès à votre réseau sans fil 36
Optimisation de la sécurité à l'aide du pare-feu intégré 37

Utilisation d'un lecteur externe

Configuration du stockage 38

Routage et déclenchement de port

Configuration du routage de port 46
Configuration du routage de port unique 46
Configuration du routage pour plusieurs ports 47
Configuration du routage d'une plage de ports 47
Configuration du déclenchement d'une plage de ports pour le jeu en ligne 48
Configuration de votre Xbox pour le jeu en ligne 49

Mise à jour et surveillance

Sauvegarde et rétablissement de la configuration de votre routeur 50
Rétablissement des valeurs par défaut 50
Mise à niveau du microcode de votre routeur 51
Vérification de l'état de votre routeur 52
Désactivation des voyants d'état des ports Ethernet 54
Test de votre connexion Internet 54
Configuration et utilisation des journaux 55

Structure des menus de l'utilitaire Web

Linksys E1550 57

Caractéristiques techniques

Linksys E1550 59

Présentation du produit

Contenu de la boîte

La boîte contient votre routeur ainsi que les accessoires suivants :

- Câble réseau (Ethernet)
- Adaptateur secteur c.a.
- CD avec logiciel de configuration du routeur et documentation

Fonctionnalités

Technologie sans fil N

Votre routeur intègre la connectivité sans fil 802.11n, une technologie de pointe qui assure une portée et des vitesses optimales. Il vous permet de créer un réseau ultra-puissant, adapté aux exigences de votre cinéma maison. Connectez vos ordinateurs, vos téléviseurs compatibles avec Internet, vos consoles de jeu, vos téléphones intelligents et autres appareils Wi-Fi et profitez d'une expérience exceptionnelle grâce aux vitesses de transfert ultra-rapides.

SpeedBoost

L'antenne de qualité supérieure contribue à garantir des vitesses de transmission élevées dans toutes les pièces de la maison. (Modèle E1500 uniquement; non disponible sur le modèle E1200)

Une sécurité de pointe

Protégez-vous des menaces sur Internet et des tentatives d'utilisation non autorisées de votre connexion Wi-Fi grâce au cryptage WPA/WPA2. Le pare-feu SPI assure la sécurité de votre réseau.

Les avantages de la technologie Fast Ethernet

Utilisez les quatre ports Fast Ethernet (10/100) pour accélérer le partage de fichiers entre vos ordinateurs et vos serveurs.

Port USB intégré

Grâce au port de stockage USB, ajoutez un lecteur USB externe à votre réseau et partagez des fichiers chez vous ou sur Internet.

Conçu pour votre réseau domestique

Connectez vos ordinateurs, imprimantes et autres appareils à votre réseau sans fil et à Internet. La technologie de qualité du service (QoS) attribue des niveaux de priorité au trafic afin d'optimiser la vitesse et les performances. Vous bénéficiez de téléchargements rapides et de séances de jeu ininterrompues.

Facile à gérer

Le logiciel Cisco Connect permet de personnaliser les paramètres et d'ajouter rapidement des périphériques à votre réseau.

Réseau distinct pour les invités

Créez un réseau distinct, sécurisé et protégé par mot de passe pour vos invités.

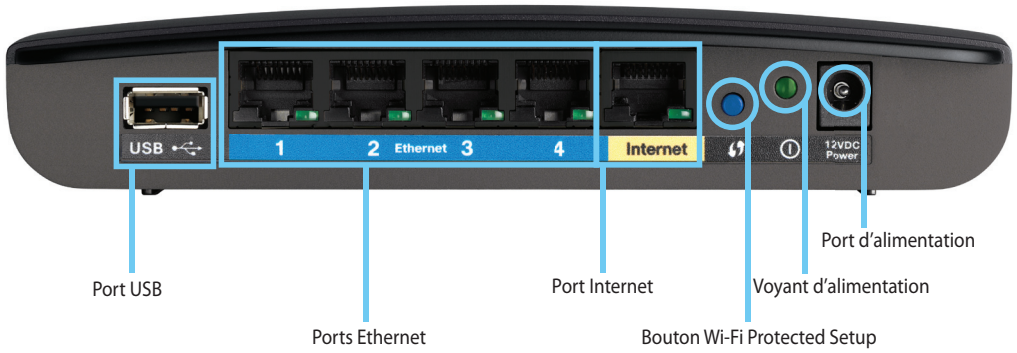
Contrôle parental

Restreignez l'accès à certaines heures et bloquez l'accès à certains sites Web.

IPv6

Supporte la dernière technologie de protocole Internet pour un réseau évolutif.

Vue arrière

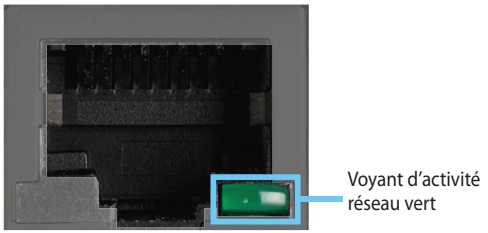


- **Port USB** : Connectez un lecteur USB pour partager facilement son contenu avec d'autres utilisateurs de votre réseau ou sur Internet. Pour en savoir davantage, reportez-vous à la section « Utilisation d'un lecteur externe », page 38.
- **Ports Ethernet** : Branchez des câbles Ethernet (également appelés câbles réseau) sur les ports bleus Gigabit (10/100/1000) pour connecter d'autres périphériques filaires Ethernet à votre réseau.
- **Port Internet** : Branchez un câble Ethernet (également appelé câble réseau ou Internet) sur le port jaune pour connecter votre modem au routeur.

  Bouton Wi-Fi Protected Setup[MC] : Appuyez sur ce bouton pour configurer facilement la sécurité sans fil des périphériques de votre réseau compatibles avec la fonction Wi-Fi Protected Setup (accès Wi-Fi protégé). Pour en savoir davantage, reportez-vous à la section « Configuration de la sécurité sans fil à l'aide de la fonction Wi-Fi Protected Setup », page 34.
- **Voyant d'alimentation** : Ce voyant reste allumé lorsque le routeur est branché à une source d'alimentation et après une connexion réussie à l'aide de la fonction Wi-Fi Protected Setup. Il clignote lentement durant le démarrage, la mise à niveau du microcode et la connexion à l'aide de la fonction Wi-Fi Protected Setup. Il clignote rapidement en cas d'erreur liée à la fonction Wi-Fi Protected Setup.
- **Alimentation** : Branchez l'adaptateur secteur c.a. fourni avec le routeur sur ce port.

ATTENTION
Utilisez exclusivement l'adaptateur fourni avec votre routeur.

Voyants d'activité des ports



Port réseau ou Internet

- **Voyant d'activité vert** : Sur un port Ethernet, le voyant s'allume lorsque le port est relié à un autre port Gigabit Ethernet au moyen d'un câble. Le voyant du port Internet s'allume lorsque le port est relié à un modem. Le voyant clignote lors du transfert de données quelque soit le type de port.

Vue de dessous

- **Bouton de réinitialisation** : Pour rétablir les valeurs par défaut du routeur, maintenez ce bouton enfoncé pendant 5 à 10 secondes (jusqu'à ce que les voyants des ports clignotent simultanément). Vous pouvez également rétablir les valeurs par défaut à l'aide de l'utilitaire Web. Pour en savoir davantage, reportez-vous à la section « Rétablissement des valeurs par défaut », page 50.

Configuration : Opérations de base

Création d'un réseau domestique

Qu'est-ce qu'un réseau?

Un réseau désigne un groupe de périphériques qui peuvent communiquer entre eux. Un réseau domestique peut également comprendre un accès à Internet, pour lequel vous aurez besoin d'un routeur tel que celui-ci.

En général, un réseau domestique se compose de plusieurs ordinateurs, d'une imprimante, d'un modem et d'un routeur. Les réseaux domestiques plus importants peuvent également comprendre un commutateur, des routeurs supplémentaires, des points d'accès et de nombreux appareils multimédias compatibles avec Internet tels que des téléviseurs, des consoles de jeu et des caméras Web.

- **Modem** : Permet de connecter un ordinateur ou un routeur à votre fournisseur d'accès Internet (FAI).
- **Routeur** : Permet de connecter vos périphériques réseau filaires et sans fil entre eux et au modem (c'est-à-dire à votre FAI).
- **Commutateur** : Permet de connecter plusieurs périphériques réseau filaires au réseau domestique. Votre routeur est doté d'un commutateur réseau intégré (les ports Ethernet). Si le nombre de périphériques réseau filaires dont vous disposez est supérieur au nombre de ports Ethernet du routeur, vous devrez vous procurer un commutateur supplémentaire pour regrouper les connexions filaires.

Installation d'un réseau domestique

1. Procurez-vous l'équipement adéquat. Si votre réseau inclut un accès à Internet, vous aurez besoin de ce qui suit :
   - Ordinateurs dotés d'un port Ethernet ou de la connectivité sans fil
   - Modem pour la connexion au FAI (souvent, le modem est fourni par le FAI)
   - Routeur pour connecter les ordinateurs entre eux et au modem
   - Accès Internet à votre domicile, fourni par un FAI (fournisseur d'accès Internet)
2. Vérifiez que votre modem fonctionne. Votre FAI peut vous aider à configurer votre modem et à vous assurer qu'il fonctionne correctement.
3. Configurez votre routeur. Reportez-vous à la section « Configuration de votre routeur », page 7.
4. Pour connecter un ordinateur ou un autre périphérique à votre réseau, reportez-vous aux sections « Connexion d'un ordinateur à votre réseau », page 10 et « Connexion d'autres périphériques », page 13.

Pour obtenir de l'aide

En complément de l'information contenue dans le présent Guide de l'utilisateur, les ressources d'aide suivantes sont à votre disposition :

- **Linksys.com/support** (documentation, téléchargements, FAQ, soutien technique, clavardage en direct, forums)
- CD de configuration (Guide de dépannage, avis juridiques et réglementaires)
- Aide de Cisco Connect, accessible en ouvrant le logiciel et en cliquant sur Learn More (en savoir plus) lorsque l'option est disponible
- Aide contextuelle de l'utilitaire Web, accessible en ouvrant l'utilitaire et en cliquant sur **Help** (aide) dans la colonne de droite

Configuration de votre routeur

Utilisez le logiciel Cisco Connect pour configurer facilement et rapidement votre routeur. Vous trouverez ce logiciel sur le CD fourni avec votre routeur. Vous pouvez également le télécharger depuis le site de soutien Linksys.com/support. Cisco Connect vous guide pas à pas dans le processus de connexion de votre routeur à votre réseau domestique. Pour commencer, reportez-vous à la section « Lancement de Cisco Connect » ci-après.

Les utilisateurs avancés peuvent configurer le routeur manuellement à l'aide de l'utilitaire Web. Pour commencer, reportez-vous à la section « Ouverture de l'utilitaire Web », page 18.

Lancement de Cisco Connect

Le logiciel de configuration de votre routeur Cisco Connect s'installe automatiquement sur votre ordinateur lorsque vous exécutez le CD. Vous pouvez ensuite utiliser le logiciel pour gérer facilement votre routeur. Pour installer Cisco Connect sur un autre ordinateur une fois le routeur configuré, reportez-vous à la section « Installation de Cisco Connect sur un autre ordinateur », page 9.

REMARQUES :
Le CD Cisco Connect ne fonctionne qu'avec ce modèle de routeur.

Si vous perdez le CD de configuration, téléchargez le logiciel depuis le site **Linksys.com/support**.

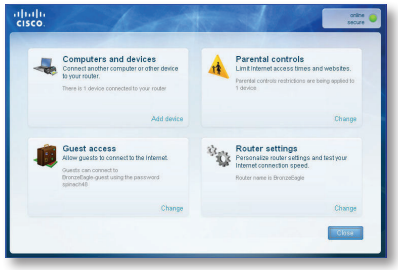
Pour lancer Cisco Connect pour la première fois :

1. Insérez le CD dans votre lecteur de CD ou DVD.
2. Cliquez sur **Set up your Linksys Router** (installer votre routeur Linksys).

   Si la fenêtre ne s'affiche pas :

   - Sous Windows, cliquez sur **Démarrer** et sur **Ordinateur**, puis double-cliquez sur le lecteur **CD** et sur l'icône **Setup** (configuration).
   - Sous Mac, double-cliquez sur l'icône de **CD** de votre bureau, puis double-cliquez sur l'icône **Setup** (configuration).
3. Suivez les instructions à l'écran pour procéder à la configuration du routeur. Une fois la configuration terminée, vous remarquerez que le logiciel Cisco Connect a été installé sur votre disque dur.

Après l'installation de Cisco Connect et la configuration du routeur, vous pouvez utiliser Cisco Connect pour gérer facilement un grand nombre de paramètres de votre routeur.



Pour lancer Cisco Connect sur un ordinateur Windows :

1. Cliquez sur **Démarrer**, sur **Programmes**, puis sur **Cisco Connect**. Le menu principal de Cisco Connect s'ouvre.

Pour lancer Cisco Connect sur un ordinateur Mac OS X :

1. Ouvrez le dossier **Applications**, puis double-cliquez sur l'icône **Cisco Connect**. Le menu principal de Cisco Connect s'ouvre.

Installation de Cisco Connect sur un autre ordinateur

Cisco Connect s'installe sur votre ordinateur lorsque vous exécutez le CD de configuration. Toutefois, vous aurez peut-être besoin de gérer votre routeur à l'aide d'un autre ordinateur de votre réseau.

ATTENTION
Une fois le routeur configuré, n'exécutez pas le CD pour installer Cisco Connect sur un autre ordinateur. Si vous exécutez de nouveau le CD de configuration, vous devrez entrer le nom de réseau du routeur (SSID) et le mot de passe.

Pour installer Cisco Connect sur un autre ordinateur :

1. Reportez-vous à la section « Connexion d'un ordinateur à l'aide de la clé de configuration facile », page 10. Une fois l'opération terminée, vous remarquerez que le logiciel Cisco Connect a été installé sur votre disque dur.

Amélioration de la vitesse de votre connexion sans fil

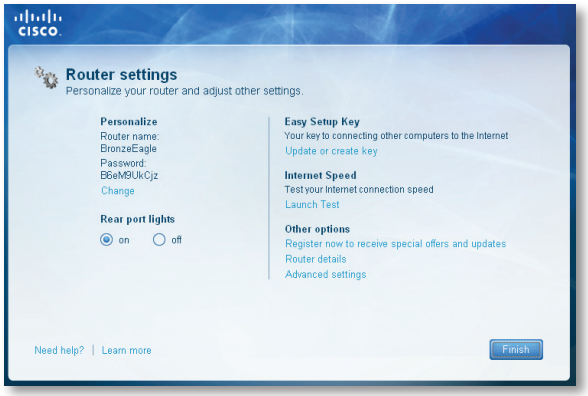
Suivez les conseils ci-après pour améliorer la vitesse de connexion sans fil de votre réseau :

- Assurez-vous que votre routeur est situé dans un emplacement adéquat.
- Pour optimiser la portée du réseau, installez le routeur au centre de votre domicile, si possible près du plafond.
- Évitez de placer le routeur sur ou à proximité d'objets métalliques (tels que des classeurs et des meubles), de surfaces réfléchissantes (surfaces en verre ou miroirs) ou de murs en maçonnerie.
- Toute obstruction, même si elle n'est pas provoquée par des objets métalliques, risque d'affaiblir le signal sans fil. Essayez de réduire au maximum les obstacles entre le routeur et le périphérique sans fil.
- Éloignez le routeur de toute lumière fluorescente, de tout moteur et de tout appareil électronique.
- Les performances du routeur sont sujettes à de nombreux facteurs environnementaux. Si le signal est faible, essayez de déplacer le routeur et testez la puissance du signal pour déterminer l'emplacement idéal.
- Si possible, mettez à niveau les interfaces de réseau sans fil (notamment les cartes de réseau sans fil des ordinateurs) afin qu'elles soient conformes à la norme 802.11n. Si l'un des périphériques sans fil de votre réseau fonctionne sur une norme plus ancienne, il risque de ralentir l'ensemble de votre réseau

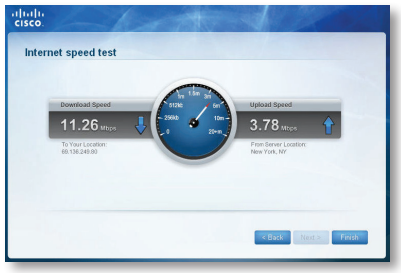
Test de la vitesse de votre connexion sans fil

Pour tester la vitesse de votre connexion sans fil :

1. Lancez Cisco Connect et cliquez sur **Change** (modifier) sous *Router settings* (paramètres du routeur). L'écran *Router settings* (paramètres du routeur) s'affiche.



2. Cliquez sur **Launch Test** (lancer le test) sous *Internet Speed* (vitesse Internet). L'écran *Internet speed test* (test de vitesse Internet) s'ouvre.
3. Suivez les instructions à l'écran pour procéder au test.



Connexion de périphériques à votre réseau

Connexion d'un ordinateur à votre réseau

Vous pouvez ajouter un ordinateur à votre réseau manuellement ou, plus simplement, à l'aide d'une clé de configuration facile.

Connexion d'un ordinateur à l'aide de la clé de configuration facile

Créez tout d'abord une clé de configuration facile à l'aide d'un lecteur USB disponible. Vous pourrez ensuite utiliser ce lecteur pour connecter plusieurs ordinateurs au réseau.

CONSEIL
La clé de configuration facile contient les données de votre réseau (nom, mot de passe, type de sécurité et clé de sécurité) et vous évite d'avoir à les mémoriser.

Pour créer une clé de configuration facile :

1. Lancez Cisco Connect, puis cliquez sur **Add device** (ajouter un périphérique) sous *Computers and devices* (ordinateurs et périphériques). L'écran *Computers and other devices* (ordinateurs et autres périphériques) s'affiche.

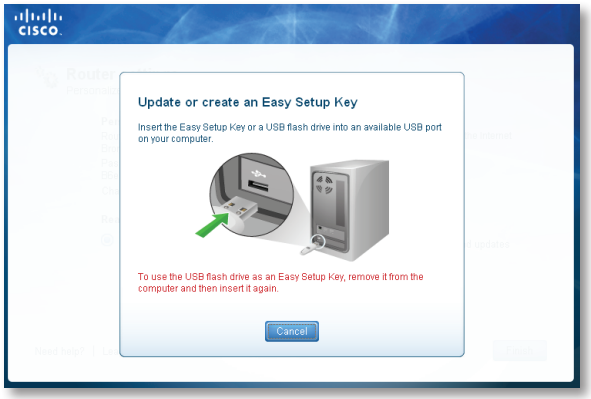
Computers and other devices
What do you want to connect to your router?
Computer
Another computer in your home
Wireless printer
A wireless printer in your home
Other wireless devices
An iPhone® smartphone, a video game console, or other wireless device
Need help?
< Back
Next >
Cancel

2. Cliquez sur **Computer** (ordinateur).

Do you have an Easy Setup Key?
The Easy Setup Key helps you connect other computers to your Linksys E4200. You may have created one using your own USB flash drive which will look different from the picture below.
Yes, I have an Easy Setup Key
No, I don't have an Easy Setup Key — create a new one now
I want to connect manually using my wireless settings
Need help?
< Back
Next >
Cancel

3. Sélectionnez **No, I don't have an Easy Setup Key** (non, je n'ai pas de clé de configuration facile), puis cliquez sur **Next** (suivant).
4. Insérez un lecteur USB dans un port USB disponible de l'ordinateur. Ce lecteur USB sera votre nouvelle clé de configuration facile.

   Cisco Connect détecte le lecteur USB que vous venez de connecter et copie les paramètres du routeur ainsi que le logiciel Cisco Connect.


Update or create an Easy Setup Key
Insert the Easy Setup Key or a USB flash drive into an available USB port on your computer.
To use the USB flash drive as an Easy Setup Key, remove it from the computer and then insert it again.
Cancel

5. Une fois les fichiers copiés sur la clé de configuration facile, retirez-la de votre ordinateur. Vous pouvez désormais installer Cisco Connect sur d'autres ordinateurs et les connecter au réseau.
6. Cliquez sur **Close** (fermer).

Pour connecter un ordinateur au réseau à l'aide de votre clé de configuration facile :

1. Lancez Cisco Connect, puis cliquez sur **Add device** (ajouter un périphérique) sous *Computers and devices* (ordinateurs et périphériques). L'écran *Computers and other devices* (ordinateurs et autres périphériques) s'affiche.
2. Cliquez sur **Computer** (ordinateur).

Do you have an Easy Setup Key?
The Easy Setup Key helps you connect other computers to your Linksys E4200. You may have created one using your own USB flash drive which will look different from the picture below.
Yes, I have an Easy Setup Key
No, I don't have an Easy Setup Key — create a new one now
I want to connect manually using my wireless settings
Need help?
< Back
Next >
Cancel

3. Sélectionnez **Yes, I have an Easy Setup Key** (oui, j'ai une clé de configuration facile), puis cliquez sur **Next** (suivant). L'écran *Connecting another computer* (connexion d'un autre ordinateur) s'affiche.
4. Insérez la clé de configuration facile dans un port USB de l'ordinateur que vous voulez connecter au réseau. L'écran *Connecting another computer* (connexion d'un autre ordinateur) s'affiche.

   Si cet écran ne s'ouvre pas, affichez les fichiers de la clé de configuration facile à l'aide de l'explorateur Windows ou du Finder et double-cliquez sur **Connect** (connexion).
5. Cliquez sur **Connect to your router** (connecter à votre routeur) et suivez les instructions à l'écran.
6. Revenez à l'ordinateur qui exécute Cisco Connect et cliquez sur **Next** (suivant).
7. Entrez le nom de l'ordinateur que vous venez d'ajouter au réseau, puis cliquez sur **Finish** (terminé).

Connexion manuelle d'un ordinateur

Pour connecter un ordinateur sans clé de configuration facile, vous devrez imprimer ou noter certaines informations.

IMPORTANT
Si vous connectez manuellement un ordinateur au réseau, Cisco Connect *ne* sera *pas* installé.

Pour connecter manuellement un ordinateur à votre réseau :

1. Lancez Cisco Connect, puis cliquez sur **Add device** (ajouter un périphérique) sous *Computers and devices* (ordinateurs et périphériques). L'écran *Computers and other devices* (ordinateurs et autres périphériques) s'affiche.

Computers and other devices
What do you want to connect to your router?
Computer
Another computer in your home
Wireless printer
A wireless printer in your home
Other wireless devices
An iPhone® smartphone, a video game console, or other wireless device
Need help?
< Back
Next >
Cancel

2. Cliquez sur **Computer** (ordinateur).
3. Sélectionnez **I want to connect manually using my wireless settings** (je veux configurer manuellement la connexion en utilisant mes paramètres de réseau sans fil), puis cliquez sur **Next** (suivant). L'écran qui s'affiche contient les paramètres de votre réseau.
4. Notez le nom du réseau (SSID), la clé de sécurité et le type de sécurité, ou cliquez sur **Print these settings** (imprimer ces paramètres) si une imprimante est connectée.
5. Entrez les paramètres dans le gestionnaire de réseau sans fil de l'ordinateur que vous souhaitez connecter.

6. Une fois l'ordinateur connecté au réseau, revenez à l'ordinateur qui exécute Cisco Connect et cliquez sur **Next** (suivant).
7. Cliquez sur **Connect to your Linksys router** (connecter à votre routeur Linksys) et suivez les instructions à l'écran.
8. Entrez le nom du nouvel ordinateur ajouté au réseau lorsqu'un message vous y invite, puis cliquez sur **Finish** (terminé).

Connexion d'une imprimante

Si vous installez une imprimante nécessitant l'utilisation d'un câble, suivez les instructions d'installation de l'imprimante. Ensuite, suivez les instructions du système d'exploitation de votre ordinateur pour partager l'imprimante sur votre réseau

Si vous installez une imprimante sans fil, vous devrez en revanche vous assurer qu'elle communique avec le routeur. Avant de tenter d'installer votre imprimante sans fil, vérifiez les points suivants :

- Toutes les étapes d'installation de l'imprimante ont été suivies, à l'exception de celles de connexion au réseau.
- Votre imprimante prend en charge la norme de cryptage sans fil WPA/WPA2.
- Si votre imprimante sans fil prend en charge la fonction WPS (Wi-Fi Protected Setup), connectez-la à votre réseau par WPS. Reportez-vous à la section « Configuration de la sécurité sans fil à l'aide de la fonction Wi-Fi Protected Setup », page 34.

Pour connecter une imprimante sans fil à votre réseau :

1. Lancez Cisco Connect, puis cliquez sur **Add device** (ajouter un périphérique) sous *Computers and devices* (ordinateurs et périphériques). L'écran *Computers and other devices* (ordinateurs et autres périphériques) s'affiche.

cisco
Computers and other devices
What do you want to connect to your router?
Computer
Another computer in your home
Wireless printer
A wireless printer in your home
Other wireless devices
An iPhone® smartphone, a video game console, or other wireless device
Need help?
< Back
Next >
Cancel

2. Cliquez sur **Wireless printer** (imprimante sans fil). L'écran qui s'affiche contient les paramètres de votre réseau.
3. Notez le nom du réseau (SSID), la clé de sécurité et le type de sécurité, ou cliquez sur **Print these settings** (imprimer ces paramètres) si une autre imprimante est déjà connectée.
4. Entrez les paramètres du réseau sans fil en suivant les instructions de votre imprimante.
5. Une fois l'imprimante connectée à votre réseau, cliquez sur **Next** (suivant) dans Cisco Connect.
6. Revenez à l'ordinateur qui exécute Cisco Connect et cliquez sur **Next** (suivant). L'écran *Name your printer* (attribution d'un nom à votre imprimante) s'affiche.
7. Entrez le nom de l'imprimante, puis cliquez sur **Finish** (terminé).
8. Pour ajouter la nouvelle imprimante à la liste des imprimantes disponibles, suivez les instructions du système d'exploitation de votre ordinateur.

Connexion d'autres périphériques

Vous pouvez connecter de nombreux types de périphériques sans fil à votre réseau domestique, notamment :

- Consoles de jeu
- Téléviseurs compatibles avec Internet et lecteurs multimédias
- Lecteurs de musique numériques
- Téléphones intelligents

En raison de la grande diversité d'appareils et de modes de connexion, vous devrez entrer manuellement les paramètres du réseau pour connecter ces périphériques au réseau.

Pour connecter manuellement un périphérique à votre réseau :

1. Lancez Cisco Connect, puis cliquez sur **Add device** (ajouter un périphérique) sous *Computers and devices* (ordinateurs et périphériques). L'écran *Computers and other devices* (ordinateurs et autres périphériques) s'affiche.

cisco
Computers and other devices
What do you want to connect to your router?
Computer
Another computer in your home
Wireless printer
A wireless printer in your home
Other wireless devices
An iPhone® smartphone, a video game console, or other wireless device
Need help?
< Back
Next >
Cancel

2. Cliquez sur **Other devices** (autres périphériques). L'écran qui s'affiche contient les paramètres de votre réseau.

3. Notez le nom du réseau (SSID), la clé de sécurité et le type de sécurité, ou cliquez sur **Print these settings** (imprimer ces paramètres) si une imprimante est connectée.

cisco
Connecting a device
An iPhone® smartphone, a video game console, or other wireless device.
1. Refer to the device's documentation to learn how to connect it to a wireless network.
2. Then, on the device, use the wireless settings below to connect the device to your router.
Network name (SSID): BronzeEagle
Security Key: B6eM9UkCjz
Security Type: WPA2 or WPA
Print these settings | Learn more
3. Click Next after you connect.
Need help?
< Back
Next >
Cancel

4. Entrez les paramètres du réseau sans fil en suivant les instructions de votre périphérique.
5. Une fois le périphérique connecté au réseau, revenez à l'ordinateur qui exécute Cisco Connect et cliquez sur **Next** (suivant).
6. Entrez le nom du périphérique, puis cliquez sur **Finish** (terminé).

Pour obtenir des instructions supplémentaires sur la connexion d'une console de jeu à votre réseau, consultez également la section :

- « Optimisation de votre routeur pour les jeux et les communications vocales », page 23
- « Configuration du routage de port », page 46
- « Configuration du déclenchement d'une plage de ports pour le jeu en ligne », page 48

Configuration du contrôle parental

Utilisez le contrôle parental de votre routeur pour :

- restreindre l'accès à Internet à certaines heures;
- bloquer certains sites Web en fonction de leur contenu;
- bloquer certains sites Web de votre choix;
- définir les restrictions ci-dessus uniquement pour certains ordinateurs.

CONSEIL
Lorsqu'un utilisateur tente d'accéder à un site Web bloqué, une fenêtre s'affiche pour demander le mot de passe de contrôle parental. Entrez le mot de passe pour accéder au contenu bloqué.

Accès au contrôle parental

Vous devez définir un mot de passe lorsque vous accédez au contrôle parental pour la première fois.

Pour accéder au contrôle parental pour la première fois :

1. Lancez Cisco Connect et cliquez sur **Change** (modifier) sous **Parental controls** (contrôle parental). L'écran *Parental controls password* (mot de passe de contrôle parental) s'affiche.

Parental controls
Parental controls allow you to limit when your children can get online and the websites they can see. To use parental controls, first create a password.
Parental controls password:
Verify password:
4 - 32 characters
Enter a secret question and answer. These will be used if you forget your password and need to reset it.
Secret question:
What was your first pet's name?
Answer:
Shadow
OK
Cancel

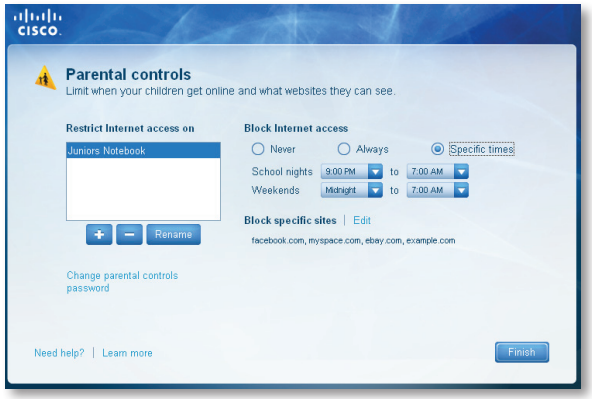
2. Entrez un mot de passe de 4 à 32 caractères, puis une question et une réponse secrètes.
   - Le mot de passe doit se composer de 4 à 32 caractères valides (A à Z, a à z et 0 à 9).
   - La réponse à la question secrète doit être difficile à deviner. Si vous oubliez votre mot de passe, vous pouvez le réinitialiser en répondant correctement à la question secrète.
3. Pour enregistrer vos paramètres, cliquez sur **OK**. L'écran principal *Parental controls* (contrôle parental) apparaît.

Pour accéder au contrôle parental après la première fois :

1. Lancez Cisco Connect et cliquez sur **Change** (modifier) sous **Parental controls** (contrôle parental). L'écran *Enter the parental controls password* (entrer le mot de passe de contrôle parental) s'affiche.
2. Entrez le mot de passe et cliquez sur **OK**.

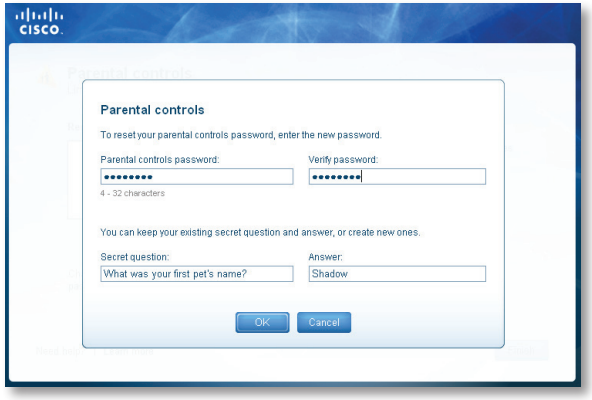
REMARQUE
Si vous oubliez le mot de passe, cliquez sur **I forgot my password** (j"ai oublié mon mot de passe) et répondez à la question secrète.

L'écran principal *Parental controls* (contrôle parental) apparaît.



Pour modifier le mot de passe de contrôle parental :

1. À l'écran principal du contrôle parental, cliquez sur **Change parental controls password** (modifier le mot de passe de contrôle parental) et suivez les instructions.

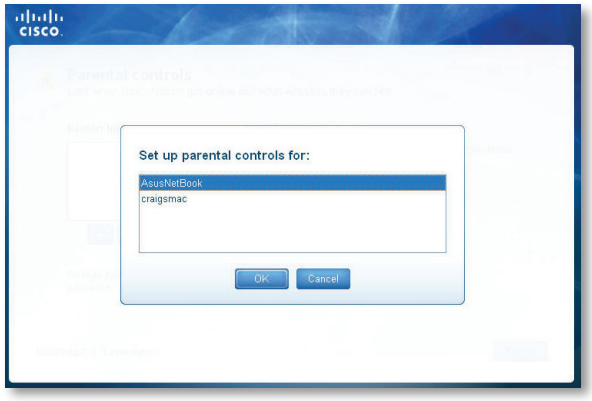


Choix des ordinateurs soumis au contrôle parental

Il n'est pas nécessaire d'appliquer le contrôle parental à tous les ordinateurs de votre réseau à domicile. Vous pouvez définir ces contrôles uniquement pour les ordinateurs auxquels les enfants ont accès.

Pour sélectionner les ordinateurs soumis au contrôle parental :

1. À l'écran principal *Parental controls* (contrôle parental), cliquez sur **+** (ajouter) sous *Restrict Internet access on* (restreindre l'accès à Internet sur).



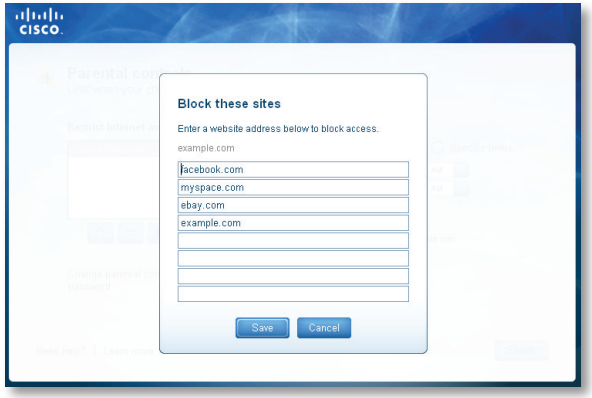
2. Cliquez sur le nom d'un ordinateur, puis sur **OK**. L'ordinateur est ajouté à la liste de ceux soumis au contrôle parental
3. Pour lever le contrôle parental sur un ordinateur, cliquez sur son nom dans la liste *Restrict Internet access on* (restreindre l'accès à Internet sur) puis sur **–** (supprimer).

Paramétrage du contrôle parental

1. À l'écran principal *Parental controls* (contrôle parental), cliquez sur le nom de l'ordinateur pour lequel vous souhaitez paramétrer le contrôle parental.
2. Sous *Block Internet access* (bloquer l'accès Internet), indiquez à quel moment l'accès Internet de l'ordinateur doit être bloqué :

- **Never** (jamais) : l'accès n'est jamais bloqué.
- **Always** (toujours) : l'accès est bloqué en tout temps.
- **Specific times** (heures particulières) : l'accès n'est bloqué qu'à certaines heures précises. Si vous sélectionnez cette option, fixez les horaires de la semaine à l'aide de l'option **School nights** (du lundi au vendredi) et de l'option **Weekends** (samedi et dimanche).

3. Pour créer une liste de sites Web à bloquer ou la modifier, cliquez sur **Edit** (modifier) à côté de *Block specific sites* (bloquer des sites spécifiques). L'écran *Block these sites* (bloquer ces sites) s'affiche.



   a. Dans une ligne vide, entrez l'adresse du site Web à bloquer.
   b. Cliquez sur **Save** (enregistrer) pour enregistrer la liste et revenir à l'écran principal *Parental controls* (contrôle parental).

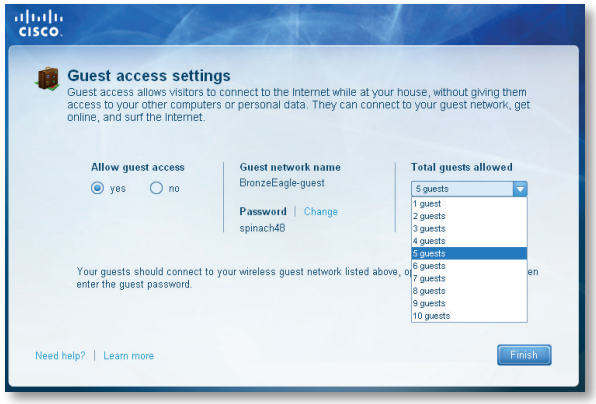
4. Cliquez sur **Finish** (terminé) pour enregistrer vos modifications.
5. Répétez les étapes ci-dessus pour chaque ordinateur devant être soumis au contrôle parental.

Configuration d'un accès d'invité

Grâce à la fonction d'accès d'invité de votre routeur, vous pouvez permettre à vos invités de se connecter à Internet tout en limitant l'accès aux autres ressources de votre réseau local. Le réseau d'invité apparaît en tant que réseau sans fil non sécurisé auquel vos invités peuvent facilement se connecter. Afin d'éviter toute utilisation non autorisée de votre accès à Internet, vos invités doivent entrer un mot de passe. Le réseau d'invité est activé par défaut.

Pour configurer un accès d'invité :

1. Lancez Cisco Connect et cliquez sur **Change** (modifier) sous *Guest Access* (accès d'invité). L'écran *Guest Access* (accès d'invité) s'affiche.



2. Sous *Allow guest access* (autoriser l'accès d'invité), cliquez sur **yes (default)** (oui, par défaut) pour activer l'accès d'invité. Pour le désactiver, cliquez sur **no** (non).
3. Veuillez noter le nom de réseau et le mot de passe du compte d'invité. Pour que vos invités puissent se connecter, vous devrez leur communiquer ces informations

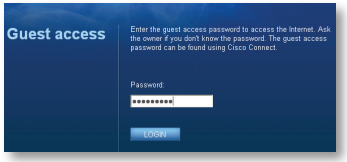
CONSEILS

Afin d'assurer la confidentialité de votre réseau d'invité, cliquez sur **Change** (modifier) pour modifier le mot de passe lorsque l'invité n'a plus besoin d'accéder au compte.

Le nom et le mot de passe du compte d'invité s'affichent à l'écran principal de Cisco Connect.

4. Dans le menu déroulant **Total guests allowed** (nombre total d'invités autorisés), sélectionnez le nombre total d'invités autorisés à se connecter simultanément au réseau.
5. Cliquez sur **Finish** (terminé) pour appliquer vos modifications.

CONSEIL
La première fois qu'un invité tente d'accéder à Internet au moyen d'un navigateur Web, la page *Guest access* (accès d'invité) s'affiche. Pour pouvoir continuer, il lui suffit d'entrer le mot de passe que vous lui avez communiqué dans le champ **Password** (mot de passe) et de cliquer sur **LOGIN** (connexion).


Guest access
Enter the guest access password to access the Internet. Ask the owner if you don't know the password. The guest access password can be found using Cisco Connect.
Password:
LOGIN

Modification du nom et du mot de passe du routeur

Vous pouvez modifier le nom et le mot de passe de votre routeur. Néanmoins, tous les périphériques sans fil connectés à ce dernier perdront leur connexion à Internet tant que vous ne les aurez pas reconnectés à l'aide du nouveau nom et du nouveau mot de passe du routeur.

ATTENTION
Si vous modifiez le nom et le mot de passe du routeur à l'aide de l'utilitaire Web, il est possible que vous ne puissiez plus gérer votre routeur à l'aide de Cisco Connect. Nous vous conseillons de suivre la procédure ci-après pour modifier les données de connexion de votre routeur.

Pour modifier le nom et le mot de passe du routeur :

1. Lancez Cisco Connect et cliquez sur **Change** (modifier) sous *Router settings* (paramètres du routeur).
2. Cliquez sur **Change** (modifier) sous *Personalize* (personnaliser). Un avertissement de modification du nom du routeur et du mot de passe s'affiche (*Changing router name and password*).

cisco
Changing router name and password
If you change the router name and password, all wireless devices connected to the router will lose their Internet connection until you reconnect them using the new name or password.
Use the Easy Setup Key to reconnect computers, and use the Computers and devices option in Cisco Connect to reconnect your other devices. You can also reconnect computers and devices manually using the new name and password.
Do you want to continue?
Yes
No

3. Cliquez sur **Yes** (oui) pour continuer.
4. Entrez le nouveau nom et le nouveau mot de passe du routeur et cliquez sur **Change** (modifier).

CONSEIL
Une fois les modifications apportées, mettez à jour votre clé de configuration facile afin de simplifier la reconnexion des autres ordinateurs au réseau.

Configuration : Avancée

Ouverture de l'utilitaire Web

Ouvrez l'utilitaire Web pour accéder à des paramètres avancés.

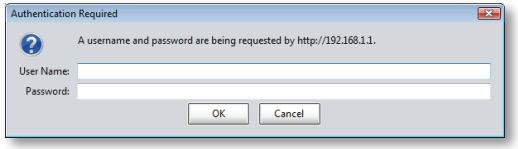
Pour ouvrir l'utilitaire Web :

1. Lancez Cisco Connect, cliquez sur **Change** (modifier) sous *Router settings* (paramètres du routeur), cliquez sur **Advanced settings** (paramètres avancés), puis sur **OK**.

   – ou –

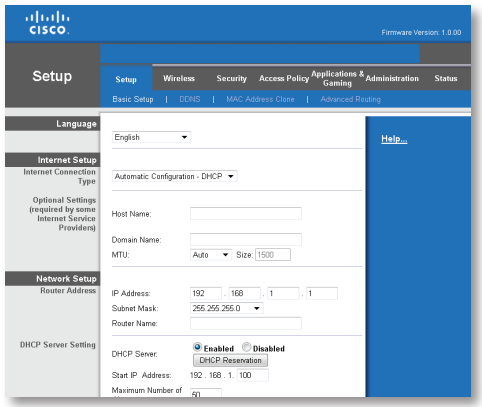
   Ouvrez un navigateur Web sur un ordinateur connecté à votre réseau, puis tapez l'adresse **192.168.1.1**.

   Le routeur vous demande un nom d'utilisateur et un mot de passe.



2. Entrez le nom et le mot de passe, puis cliquez sur **OK**. Le menu principal de l'utilitaire s'affiche.

CONSEIL
Si vous avez configuré votre routeur sans utiliser Cisco Connect, son mot de passe par défaut est **admin**. (N'entrez rien dans le champ de nom d'utilisateur.)

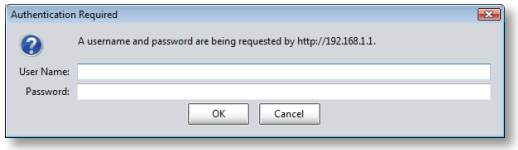


Configuration manuelle de votre routeur

Bien qu'il soit plus simple d'utiliser Cisco Connect pour configurer et gérer votre routeur, les utilisateurs avancés préféreront peut-être opter pour une configuration manuelle. Soyez vigilant lorsque vous modifiez des paramètres en employant cette méthode.

Pour configurer manuellement votre routeur :

1. Si vous avez commencé la procédure de configuration dans Cisco Connect, quittez Cisco Connect.
2. Branchez l'adaptateur secteur de votre routeur sur une prise de courant.
3. Connectez un câble Ethernet à l'un des ports bleus **Ethernet** numérotés au dos du routeur. Branchez l'autre extrémité du câble à l'ordinateur.
4. Ouvrez un navigateur Web sur l'ordinateur et entrez l'adresse **192.168.1.1**. Une fenêtre de connexion s'affiche.



5. Entrez le mot de passe par défaut (**admin**). (N'entrez rien dans le champ de nom d'utilisateur.) L'utilitaire Web s'ouvre et affiche le menu principal.
6. Une fois les paramètres modifiés, cliquez sur **Save Settings** (enregistrer les paramètres) au bas de l'écran.
7. Pour quitter l'utilitaire Web, fermez la fenêtre du navigateur Web.

CONSEIL
Pour voir la description des champs, cliquez sur **Help** (aide) à droite de l'écran.

Configuration manuelle de votre connexion Internet

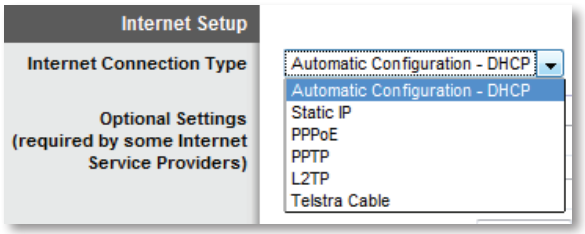
Dans la plupart des cas, Cisco Connect configure automatiquement votre connexion Internet (reportez-vous à la section « Lancement de Cisco Connect », page 8). Dans le cas de certains *FAI* (fournisseurs d'accès Internet), plus particulièrement ceux situés hors des États-Unis, vous devrez peut-être configurer manuellement la connexion Internet de votre routeur. Votre routeur prend en charge six types de connexions Internet.

Pour configurer manuellement la connexion Internet de votre routeur :

Setup (configuration) > Basic Setup (configuration de base)

1. Accédez à l'utilitaire Web (reportez-vous à la section « Ouverture de l'utilitaire Web », page 18).
2. Cliquez sur l'onglet **Setup** (configuration), puis sur la page **Basic Setup** (configuration de base).
3. Dans la liste déroulante **Internet Connection Type** (type de connexion Internet), cliquez sur le type de connexion Internet indiqué par votre FAI.

CONSEIL
Pour voir la description des champs, cliquez sur **Help** (aide) à droite de l'écran.



4. Remplissez les champs requis par votre FAI.
5. Remplissez les champs *Optional Settings* (paramètres facultatifs) uniquement si votre FAI l'exige.
6. Cliquez sur **Save Settings** (enregistrer les paramètres) au bas de la page.

Paramètres de connexion Internet IPv6

IPv6 est le dernier protocole Internet en date qui utilise des en-têtes de paques simplifiées et requiert IPSec.

Il fournit un support amélioré pour les appareils mobile IP et l'informatique. La configuration d'IPv6 est disponible sous l'onglet **Setup** (configuration).

REMARQUE
Pour utiliser les paramètres de connexion Internet IPv6 de votre routeur, le service IPv6 de votre FAI (fournisseur d'accès Internet) est requis. Pour plus d'informations sur ce service, consultez votre FAI.

Pour configurer manuellement les paramètres IPv6:

Setup *(configuration)>IPv6 Setup (Configuration IPv6)*

1. Accédez à l'utilitaire Web (reportez-vous à la section « Ouverture de l'utilitaire Web », page 18).
2. Cliquez sur l'onglet **Setup** (configuration), puis cliquez sur la page **IPv6 Setup** (configuration IPv6)
3. **IPv6-Automatique** - Sélectionnez **Enabled** (Activé) pour utiliser automatiquement IPv6 pour toutes les adresses réseau. Cette option est désactivée par défaut
4. **6rd-tunnel -** (tunnel 6rd) cette option permet à votre routeur d'envoyer des adresses IPv6 au travers de réseaux IPv4. Pour activer cette option, l'**IPv6 - automatique** doit être réglé sur **Désactivé.** Pour laisser votre routeur gérer les paramètres du tunnel 6RD (comme les préfixes et les masques d'adresse), laisser le réglage du tunnel 6RD sur **Automatic Configuration** (configuration automatique). Sélectionnez **Manual Configuration** (configuration manuelle) pour modifier ces paramètres manuellement.
   - **Prefix** - Entrez l'addresse du préfixe utilisé pour le tunnel fourni par votre FAI
   - **Prefix length** (longueur du préfixe) - Entrez la longueur du préfixe utilisé pour le tunnel fourni par votre FAI
   - **Border Relay** (Relias frontière) - Saisissez l'adresse du relais frontière utilisé pour le tunnel fourni par votre FAI
   - **IPv4 Mask Address** (Masque d'adresse IPv4) - Saisissez la longueur du masque d'adresse IPv4 utilisé pour le tunnel fourni par votre FAI
5. Cliquez sur **Save Settings** (Enregistrer les paramètres) en bas de la page

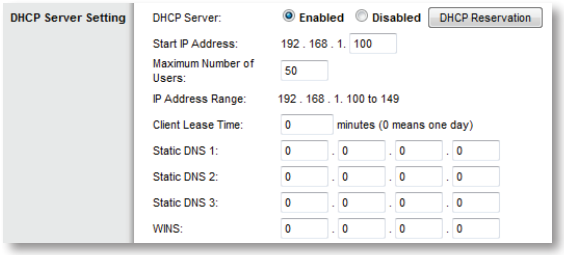
Configuration du serveur DHCP sur votre routeur

Votre routeur peut faire office de serveur *DHCP* (Dynamic Host Configuration Protocol) et attribuer une adresse IP à chaque ordinateur ou périphérique de votre réseau. Le serveur DHCP est activé par défaut. Si votre réseau est déjà doté d'un serveur DHCP, ou si vous ne souhaitez pas utiliser votre routeur en tant que serveur DHCP, désactivez ce paramètre.

Pour configurer les paramètres de serveur DHCP de votre routeur :

Setup (configuration) > Basic Setup (configuration de base) > DHCP Server Settings (paramètres du serveur DHCP)

1. Accédez à l'utilitaire Web (reportez-vous à la section « Ouverture de l'utilitaire Web », page 18).
2. Cliquez sur l'onglet **Setup** (configuration), puis sur la page **Basic Setup** (configuration de base).
3. Passez en revue les champs *DHCP Server Setting* (paramètres du serveur DHCP) au centre de l'écran. Vous pouvez :
   - activer ou désactiver le serveur DHCP;
   - modifier l'adresse de départ du serveur DHCP;
   - modifier le nombre d'utilisateurs (253 au maximum).
4. Si vous modifiez des paramètres, cliquez sur **Save Settings** (enregistrer les paramètres) au bas de la page.



CONSEIL
Pour voir la description des champs, cliquez sur **Help** (aide) à droite de l'écran.

Configuration de la réservation DHCP

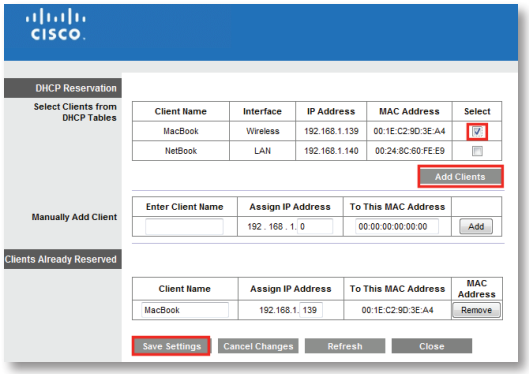
Pourquoi utiliser cette fonction? L'option *DHCP reservation* (réservation DHCP) vous permet d'attribuer une adresse IP fixe et unique à un périphérique donné de votre réseau. Cette opération permet de gérer efficacement les périphériques tels que les serveurs d'impression, les caméras Web, les imprimantes réseau et les consoles de jeu. Il est également recommandé d'attribuer une adresse IP fixe si vous souhaitez utiliser le routage de port pour les périphériques qui reçoivent du trafic entrant depuis Internet (« Configuration du routage de port », page 46).

Pour configurer la réservation DHCP :

Setup (configuration) > Basic Setup (configuration de base) > DHCP Reservation (réservation DHCP)

1. Accédez à l'utilitaire Web (reportez-vous à la section « Ouverture de l'utilitaire Web », page 18).
2. Cliquez sur l'onglet **Setup** (configuration), puis sur la page **Basic Setup** (configuration de base).
3. Cliquez sur **DHCP Reservation** (réservation DHCP) au centre de l'écran.
4. Cliquez sur **Select** (sélectionner) à côté du client pour lequel vous voulez créer une réservation DHCP.
5. Cliquez sur **Add Clients** (ajouter des clients). Le client sélectionné est ajouté au tableau *Clients Already Reserved* (clients déjà réservés).

   Vous pouvez également créer une réservation DHCP en entrant manuellement un nom de client, une adresse IP et l'adresse MAC d'un périphérique.
6. Cliquez sur **Save Settings** (enregistrer les paramètres).



CONSEIL
Pour voir la description des champs, cliquez sur **Help** (aide) à droite de l'écran.

Localisation de votre réseau sur Internet

Pourquoi aurais-je besoin de trouver mon réseau sur Internet? Vous pouvez avoir besoin de trouver votre réseau sur Internet si vous souhaitez accéder à un lecteur USB connecté à votre routeur ou à une caméra Web.

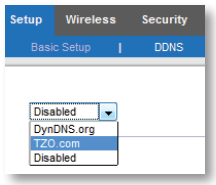
Si vous faites appel aux services de fournisseurs DDNS, la fonctionnalité DDNS de votre routeur vous permet de configurer un nom de domaine pour votre réseau, que vous pouvez ensuite utiliser pour trouver facilement votre réseau sur Internet. Si votre FAI modifie l'adresse IP de votre réseau, les fournisseurs d'accès DDNS détectent le changement d'adresse et continuent l'acheminement de votre nom de domaine vers cette adresse.

CONSEIL
Avant de configurer la fonction DDNS de votre routeur, vous devez vous abonner à un service DDNS auprès d'un fournisseur pris en charge par votre routeur.

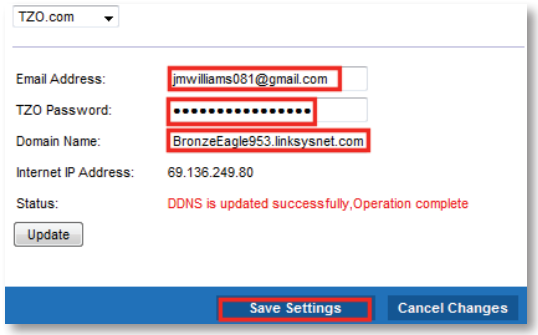
Pour configurer la fonction DDNS :

Setup (configuration) > DDNS

1. Abonnez-vous à un service DDNS sur **www.dyndns.org** ou **www.tzo.com**.
2. Accédez à l'utilitaire Web (reportez-vous à la section « Ouverture de l'utilitaire Web », page 18).
3. Cliquez sur l'onglet **Setup** (configuration), puis sur la page **DDNS**.
4. Dans la liste déroulante **DDNS Service** (service DDNS), cliquez sur votre fournisseur de service DDNS. Les exemples ci-dessous sont basés sur TZO.com. Les paramètres utilisés par DynDNS.org sont légèrement différents.



5. Remplissez les champs à l'aide des informations fournies par votre fournisseur DDNS, puis cliquez sur **Save Settings** (enregistrer les paramètres). Le champ *Status* (état) indique les mesures prises.



Dans cet exemple, le nom de domaine enregistré auprès de TZO.com est *BronzeEagle953.linksysnet.com*. Si une caméra Web a été configurée (reportez-vous à la section « Configuration du routage de port unique », page 46), vous pouvez y accéder en tapant le nom de domaine dans la barre d'adresse de votre navigateur Web, suivie du numéro de port utilisé pour la caméra. Par exemple, si la caméra utilise le port 1024, l'URL sera :

BronzeEagle953.linksysnet.com:1024

Clonage d'adresse MAC

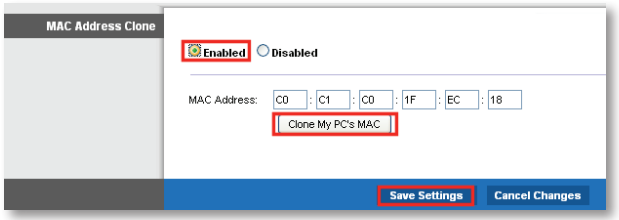
Sur tous les réseaux domestiques, une adresse *MAC* (Media Access Control) unique est attribuée à chaque périphérique. Certains FAI enregistrent l'adresse MAC du périphérique (généralement un routeur ou un ordinateur) directement connecté au modem. Si l'adresse MAC de votre ordinateur est enregistrée auprès de votre FAI et que vous ne voulez pas annuler l'enregistrement, vous pouvez *cloner* l'adresse (c'est-à-dire attribuer l'adresse MAC de l'ancien périphérique enregistrée au nouveau routeur). Si vous voulez utiliser l'adresse MAC d'un ancien routeur pour un nouveau routeur, vous devez tout d'abord identifier l'adresse MAC de l'ancien routeur, puis l'entrer manuellement dans le nouveau routeur.

REMARQUE
De nombreux FAI fournissent des adresses IP dynamiques automatiquement. L'adresse MAC du modem est donc à chaque fois réinitialisée en même temps que le modem. Si vous installez ce routeur pour la première fois, réinitialisez votre modem avant de connecter le routeur au modem. Pour réinitialiser votre modem, débranchez-le pendant environ une minute, puis rebranchez-le.

Pour cloner l'adresse MAC de votre ordinateur :

Setup (configuration) > MAC Address Clone (clonage d'adresse MAC)

1. Accédez à l'utilitaire Web (reportez-vous à la section « Ouverture de l'utilitaire Web », page 18).
2. Cliquez sur l'onglet **Setup** (configuration), puis sur la page **MAC Address Clone** (clonage d'adresse MAC).
3. Cliquez sur **Enabled** (activé).
4. Cliquez sur **Clone My PC's MAC** (cloner l'adresse MAC de mon PC) ou entrez l'adresse MAC à 12 chiffres de votre ancien routeur.
5. Cliquez sur **Save Settings** (enregistrer les paramètres).



Connexion au réseau de votre bureau à l'aide d'un VPN

Qu'est-ce qu'un VPN, et dois-je modifier les paramètres de mon routeur pour m'y connecter? Un *VPN* (Virtual Private Network, ou réseau privé virtuel) est un réseau qui utilise un réseau public, tel qu'Internet, pour fournir des communications sécurisées entre un ordinateur distant et un autre réseau. Les entreprises mettent souvent à la disposition de leurs employés un accès VPN à leurs réseaux, de sorte que ces derniers puissent travailler de chez eux ou en déplacement. La plupart des VPN d'entreprise permettent aux employés de se connecter au réseau d'entreprise à distance par l'intermédiaire Internet.

En général, l'entreprise installe une passerelle VPN sur son réseau. Les employés autorisés à travailler à distance se connectent à la passerelle VPN par Internet, à l'aide d'un logiciel de VPN et de dispositifs de sécurité fournis par l'employeur. Pour assurer une connexion sécurisée et restreindre l'accès uniquement aux utilisateurs autorisés, des mesures de sécurité et d'authentification strictes sont mises en œuvre.

Les paramètres de VPN par défaut de votre routeur ont été configurés de sorte à autoriser les protocoles de VPN les plus courants. Par conséquent, vous n'aurez généralement pas à les modifier.

Pour modifier les paramètres d'intercommunication VPN :

Security (sécurité) > VPN Passthrough (intercommunication VPN)

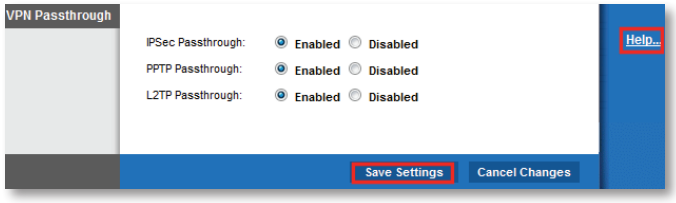
1. Accédez à l'utilitaire Web (reportez-vous à la section « Ouverture de l'utilitaire Web », page 18).
2. Cliquez sur l'onglet **Security** (sécurité), puis sur la page **VPN Passthrough** (intercommunication VPN).
3. Sélectionnez les paramètres que vous souhaitez modifier.

CONSEIL
Pour obtenir de courtes descriptions des champs de paramètres d'intercommunication VPN, cliquez sur **Help** (aide) à droite de l'écran. Vous trouverez ci-contre des descriptions plus exhaustives.

- **IPSec Passthrough** (connexion IPSec) : Le protocole *IPSec* (Internet Protocol Security, ou protocole de sécurité Internet) est utilisé pour sécuriser l'échange de paquets IP au niveau de la couche IP. Les clients VPN du réseau local peuvent créer des tunnels VPN IPSec. Cette option est activée par défaut.

- **PPTP Passthrough** (connexion PPTP) : Le *protocole PPTP* (Point-to-Point Tunneling Protocol, ou protocole de tunnel point à point) permet d'établir une connexion point à point (*PPP*) par l'intermédiaire d'un réseau IP. Les clients VPN du réseau local peuvent créer des tunnels VPN PPTP. Cette option est activée par défaut.
- **L2TP Passthrough** (connexion L2TP) : Le *protocole L2TP* (Layer 2 Tunneling Protocol, ou protocole de tunnellisation de couche 2) est utilisé pour permettre des sessions point à point sur Internet au niveau de la couche 2. Les clients VPN du réseau local peuvent créer des tunnels VPN L2TP. Cette option est activée par défaut.

4. Cliquez sur **Save Settings** (enregistrer les paramètres) pour conserver les modifications.



Optimisation de votre routeur pour les jeux et les communications vocales

Comment mon routeur régule-t-il le trafic vers Internet? Votre routeur est doté de paramètres *QoS* (qualité du service) qui régulent le trafic transmis de votre réseau vers Internet. Il est possible d'améliorer les performances pour les applications en temps réel exigeantes comme les jeux en ligne, la diffusion de vidéos, la vidéoconférence et la voix sur IP.

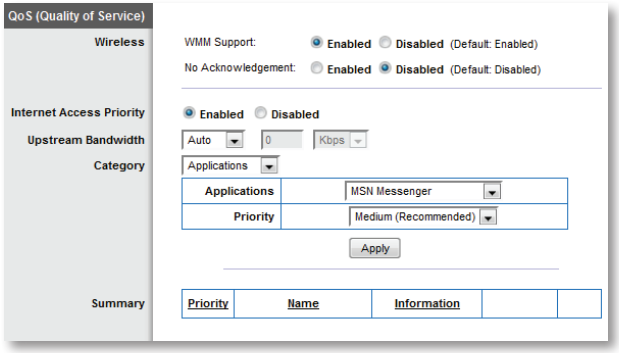
La qualité du service ne s'applique qu'au trafic transmis vers Internet. Le routeur ne contrôle pas la qualité du trafic dès lors qu'il atteint Internet.

CONSEIL
Pour en savoir plus sur l'optimisation du routeur pour le jeu en ligne, reportez-vous à la section « Routage et déclenchement de port », page 46.

Pour configurer la qualité du service :

Applications & Gaming (applications et jeux) > QoS (qualité du service)

1. Accédez à l'utilitaire Web (reportez-vous à la section « Ouverture de l'utilitaire Web », page 18).
2. Cliquez sur l'onglet **Applications & Gaming** (applications et jeux), puis sur la page **QoS** (qualité du service).



CONSEIL
Pour voir la description des champs, cliquez sur **Help** (aide) à droite de l'écran.

3. Pour mieux gérer le niveau de priorité des périphériques qui prennent en charge WMM, sélectionnez **Enabled** (activé) sous *WMM Support* (prise en charge WMM). Sinon, sélectionnez **Disabled** (désactivé).

CONSEIL
La prise en charge WMM (Wi-Fi MultiMedia) désigne une fonctionnalité de qualité du service sans fil basée sur la norme IEEE 802.11e. Elle améliore la qualité des applications audio, vidéo et vocales en régulant le niveau de priorité du trafic sans fil. Pour pouvoir bénéficier de cette fonctionnalité, les périphériques clients sans fil de votre réseau doivent également prendre en charge WMM.

4. Pour que le routeur renvoie les données en cas d'erreur, sélectionnez **Disabled** (désactivé) sous *No Acknowledgement* (aucune confirmation). Sinon, sélectionnez **Enabled** (activé).

5. Pour définir les priorités d'accès pour des applications ou périphériques particuliers, sélectionnez **Enabled** (activé) à côté de *Internet Access Priority* (priorité d'accès Internet).
6. Dans la liste déroulante **Category** (catégorie), sélectionnez le type d'élément pour lequel vous voulez définir une priorité. La liste des éléments installés correspondant à la description s'affiche.

CONSEIL
Ne réglez pas toutes les priorités sur **High** (élevée). Si tous les éléments sont associés au même niveau de priorité, vous obtiendrez le même résultat que si vous désactiviez la fonction Internet Access Priority (priorité d'accès Internet).

- **Applications** et **Online Games** (jeux en ligne) : Ces options permettent d'attribuer un niveau de priorité pour une application ou un jeu en ligne.
  a) Sélectionnez l'application ou le jeu en ligne à ajouter dans la liste déroulante, puis définissez la priorité.
  b) Cliquez sur **Apply** (appliquer), puis sur **Save Settings** (enregistrer les paramètres).

CONSEIL
Avant d'ajouter un nouveau jeu ou une nouvelle application, vous devez connaître le port et le protocole utilisés (pour en savoir plus, consultez la documentation de l'application ou du jeu).

- **MAC Address** (adresse MAC) et **Voice Device** (périphérique vocal) : Ces options vous permettent de réguler le trafic en fonction du périphérique qui accède au réseau. Par exemple, si vous souhaitez que votre console de jeu accède en priorité à Internet par rapport à votre ordinateur, attribuez une priorité plus élevée à la console à l'aide de son adresse MAC. Il est recommandé d'attribuer une priorité élevée à tous les périphériques vocaux.
  a) Sélectionnez **MAC Address** (adresse MAC) ou **Voice Device** (périphérique vocal) dans la liste déroulante, puis entrez le nom du périphérique à ajouter.
  b) Entrez l'adresse MAC à 12 chiffres du périphérique, puis sélectionnez la priorité.
  c) Cliquez sur **Apply** (appliquer), puis sur **Save Settings** (enregistrer les paramètres).

CONSEIL
Vous trouverez généralement l'adresse MAC à 12 chiffres du périphérique au-dessous de celui-ci. Si le périphérique est connecté au réseau et sous tension, cliquez sur l'onglet **Administration** de l'utilitaire Web du routeur et cliquez sur la page **Local Network** (réseau local), puis sur **DHCP Client Table** (table des clients DHCP).

7. Configurez l'option **Upstream Bandwidth** (bande passante montante).
   - Pour permettre au routeur de détecter la bande passante maximum, sélectionnez l'option par défaut **Auto**. L'option Auto définit les vitesses par multiples de 512 kbits/s.
   - Pour choisir le maximum, sélectionnez **Manual** (manuel), puis sélectionnez la bande passante à utiliser.

ATTENTION
Si vous définissez une bande passante maximum trop élevée, le routeur ne pourra pas appliquer correctement les niveaux de priorité et des problèmes de qualité du service risquent de survenir.

8. Une fois les niveaux de priorités définis, cliquez sur **Save Settings** (enregistrer les paramètres).

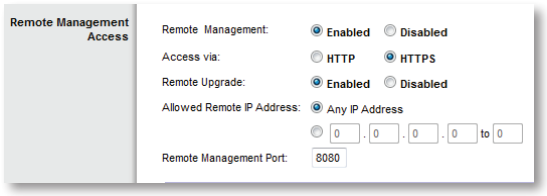
Modification à distance des paramètres du routeur

Pourquoi modifier à distance les paramètres du routeur? Vous aurez parfois besoin de modifier les paramètres de contrôle parental ou d'accès aux fichiers à distance lorsque vous n'êtes pas chez vous.

Pour configurer l'accès distant :

Administration > Management (gestion)

1. Accédez à l'utilitaire Web (reportez-vous à la section « Ouverture de l'utilitaire Web », page 18).
2. Cliquez sur l'onglet **Administration**, cliquez sur la page **Management** (gestion) et trouvez les paramètres *Remote Management Access* (accès de gestion à distance) au centre de l'écran.
3. Sélectionnez **Enabled** (activé) pour l'option *Remote Management* (gestion à distance).
4. Réglez l'option *Access via* (accès par) sur **HTTP** (par défaut) ou sur **HTTPS** si vous voulez chiffrer les données transmises par *SSL* (Secure Socket Layer) afin de renforcer la sécurité.
5. Pour pouvoir mettre à niveau le microcode de votre routeur à distance, sélectionnez **Enabled** (activé) à côté de *Remote Upgrade* (mise à niveau à distance).
6. Pour permettre l'accès à distance où que vous soyez sur Internet, sélectionnez l'option par défaut **Any IP Address** (toute adresse IP) à côté de *Allowed Remote IP Address* (autoriser l'adresse IP à distance). Sinon, entrez une plage d'adresses IP autorisées.
7. Pour l'option *Remote Management Port* (port de gestion à distance), conservez le paramètre **8080** par défaut, à moins qu'un périphérique de votre réseau utilise déjà le port 8080 (par exemple une caméra Web).
8. Cliquez sur **Save Settings** (enregistrer les paramètres) au bas de l'écran pour confirmer les modifications.


Remote Management Access
Remote Management: Enabled Disabled
Access via: HTTP HTTPS
Remote Upgrade: Enabled Disabled
Allowed Remote IP Address: Any IP Address
0 . 0 . 0 . 0 to 0
Remote Management Port: 8080

9. Cliquez sur l'onglet **Administration** puis cliquez sur la page **Management** (gestion). Notez l'adresse IP Internet (*Internet IP Address*) et le paramètre de l'option *Remote Management Port* (port de gestion à distance). Ces informations vous permettront d'accéder à votre routeur à distance.

Pour accéder à votre routeur à distance :

1. Ouvrez un navigateur Web et entrez l'adresse Internet de votre routeur. Ensuite, appuyez sur **Entrée**.
   - Si vous avez sélectionné **HTTP** pour l'option *Access via* (accès par), entrez **http://** puis l'adresse IP.

   – OU –

   - Si vous avez sélectionné **HTTPS** pour l'option *Access via* (accès par) ci-dessus, entrez **https://** puis l'adresse IP.
2. Ajoutez le signe des deux points (**:**), puis le *numéro de port de gestion à distance*. Exemple :

   https://69.192.16.170:8080

CONSEIL
Si vous activez l'option Dynamic Domain Name Service (DDNS) (reportez-vous la section « Localisation de votre réseau sur Internet », page 21), vous pouvez taper votre nom de domaine au lieu de l'adresse IP Internet du routeur. Par exemple : **https://BronzeEagle953.linksysnet.com:8080**

Entrez votre nom d'utilisateur et votre mot de passe. Utilisez les mêmes données de connexion que celles permettant d'accéder à votre routeur chez vous.

Une fois connecté à distance à l'utilitaire Web de votre routeur, vous pouvez modifier n'importe quel paramètre du routeur comme vous le feriez depuis votre réseau local.

Activation de la voix sur IP sur votre réseau

Dois-je configurer la voix sur IP? La technologie de voix sur IP, ou *VoIP* (Voice over Internet Protocol), permet d'utiliser Internet en tant qu'interface de communication téléphonique. Pour bénéficier de la voix sur IP, vous devez ouvrir un compte auprès d'un fournisseur de services VoIP. En général, ce dernier vous fournit un adaptateur téléphonique que vous devrez connecter à votre réseau. Si vous ne passez pas d'appels téléphoniques au moyen de votre réseau, inutile de modifier les paramètres par défaut.

La fonctionnalité de passerelle de couche d'application *ALG* (Application Layer Gateway) du protocole d'ouverture de session *SIP* (Session Initiation Protocol) permet aux paquets SIP, utilisés par certains fournisseurs de services VoIP, de traverser le pare-feu du routeur.

Configuration du routeur pour la voix sur IP :

Administration > Management (gestion)

1. Accédez à l'utilitaire Web (reportez-vous à la section « Ouverture de l'utilitaire Web », page 18).
2. Cliquez sur l'onglet **Administration** puis sur la page **Management** (gestion).
3. Si votre fournisseur de services VoIP utilise le protocole SIP, sélectionnez **Enabled** (activé) pour l'option *SIP ALG*.

   – OU –

   Si votre fournisseur de services VoIP utilise d'autres solutions pour traverser le NAT, par exemple les protocoles *STUN* (Session Traversal Utilities for NAT), *TURN* (Traversal Using Relay NAT) ou *ICE* (Interactive Connectivity Establishment), conservez le paramètre par défaut **Disabled** (désactivé).

REMARQUE
Vous devrez peut-être communiquer avec votre fournisseur de services VoIP afin de connaître le type de configuration utilisée pour traverser le NAT.

Configuration de la fonction UPnP

Qu'est-ce que la fonction UPnP? La fonction *UPnP* (Universal Plug and Play) permet aux périphériques d'un réseau de se détecter mutuellement et de créer automatiquement des configurations de travail. Les caméras Web, les applications de jeu et les périphériques VoIP, par exemple, sont compatibles avec la technologie UPnP. L'option UPnP est activée par défaut.

Pour configurer la fonction UPnP :

Administration > Management (gestion)

1. Accédez à l'utilitaire Web (reportez-vous à la section « Ouverture de l'utilitaire Web », page 18).
2. Cliquez sur l'onglet **Administration** puis sur la page **Management** (gestion).
3. Pour utiliser la fonction UPnP, conservez le paramètre par défaut **Enabled** (activé) à côté de l'option *UPnP*. Sinon, sélectionnez **Disabled** (désactivé).
4. Pour autoriser la modification des paramètres du routeur lorsque vous utilisez la fonction UPnP, conservez le paramètre par défaut **Enabled** (activé) pour l'option *Allow Users to Configure* (configuration par utilisateurs autorisée). Sinon, sélectionnez **Disabled** (désactivé).
5. Pour éviter que les utilisateurs du réseau local ne désactivent la connexion à Internet par UPnP, conservez le paramètre par défaut **Disabled** (désactivé) pour l'option *Allow Users to Disable Internet Access* (autoriser les utilisateurs à interdire l'accès Internet). Sinon, sélectionnez **Enabled** (activé).

Utilisation d'un routeur en tant que point d'accès

Puis-je utiliser mon nouveau routeur en tant que point d'accès? Si la zone à couvrir est relativement étendue ou si le signal est faible dans certaines pièces de votre domicile en raison d'interférences, vous pouvez utliser votre nouveau routeur pour accroître la portée de votre réseau sans fil de votre ancien routeur.

Pour configurer votre nouveau routeur comme point d'accès:

Setup>Basic Setup (Configuration>Configuration de base)

1. Utilisez un câble réseau pour connecter le port internet de ce routeur au port Ethernet ou LAN du routeur qui est connecté à votre modem.
2. Accédez à l'utilitaire Web (reportez-vous à la section « Ouverture de l'utilitaire Web », page 18).
3. Cliquez sur l'onglet **Setup** (Configuration), puis cliquez sur la page **Basic Setup** (configuration de base).
4. Pour le type de connexion Internet, sélectionnez le mode **Bridge** (pont)
5. Cliquez sur **Save Settings** (enregistrer les paramètres) pour confirmer les changements. La nouvelle adresse IP du routeur utilisé en tant que point d'accès est obtenue à partir du routeur qui est connecté à votre modem.

IMPORTANT

En mode pont, l'accès aux onglets suivants à partir de l'utilitaire Web sera indisponible :

- onglet Setup (Configuration): configuration IPv6, DDNS, Clonage d'adresse MAC, le routage avancé
- onglet Sécurité: toutes les pages
- omglet Restrictions d' accès: toutes les pages
- onglet Applications & Gaming: toutes les pages
- onglet Administration: Log (Journal)

Comment puis-je utiliser mon ancien routeur comme point d'accès? Si vous avez une grande surface à couvrir avec votre signal sans fil, ou si une partie de votre maison a des signaux faibles à cause d'interférences, vous pouvez utiliser votre ancien routeur pour étendre la portée de votre réseau sans fil. Il s'agit d'un processus complexe, si cette procédure suppose que vous avez quelques connaissances en réseautique.

CONSEIL

Consultez la documentation de votre ancien routeur. Selon la marque, les routeurs sont dotés d'un commutateur à l'extérieur du boîtier ou peuvent être convertis en point d'accès à l'aide d'un logiciel. Si l'une ou l'autre de ces options est disponible, suivez les instructions relatives à votre ancien routeur pour le transformer en point d'accès.

Vous devrez noter les paramètres de votre nouveau routeur afin d'appliquer certains d'entre eux à l'ancien routeur.

Pour afficher les paramètres de votre nouveau routeur :

Wireless (sans fil) > Basic Wireless Settings (paramètres de base du réseau sans fil)
Wireless (sans fil) > Wireless Security (sécurité du réseau sans fil)
Status (état) > Wireless Network (réseau sans fil)
Setup (configuration) > Basic Setup (configuration de base)

1. Assurez-vous que votre nouveau routeur est connecté à Internet.
2. Dans l'utilitaire Web, cliquez sur l'onglet **Wireless** (sans fil), puis sur la page **Basic Wireless Settings** (paramètres de base du réseau sans fil). Notez le *nom de réseau (SSID)*.
3. Cliquez sur l'onglet **Wireless** (sans fil), puis sur la page **Wireless Security** (sécurité du réseau sans fil). Notez le *mode de sécurité* et la phrase de vérification.
4. Cliquez sur l'onglet **Status** (état), puis sur la page **Wireless Network** (réseau sans fil). Notez le *canal*.
5. Cliquez sur l'onglet **Setup** (configuration), puis sur la page **Basic Setup** (configuration de base). Notez la plage d'adresses IP (par défaut, 192.168.1.100 à 192.168.1.149) du serveur DHCP.

Pour utiliser votre ancien routeur en tant que point d'accès :

1. Connectez l'ancien routeur à votre ordinateur et accédez à son utilitaire d'administration Web.

REMARQUE

Enregistrez vos modifications après chacune des étapes ci-dessous.

2. Ouvrez la page de configuration du réseau local (LAN) .

3. Dans le champ **Router IP address** (adresse IP du routeur), entrez une adresse IP inutilisée sur le réseau local pour votre nouveau routeur.

   Par exemple, si votre nouveau routeur utilise l'adresse IP 192.168.1.1, choisissez une adresse IP sur le réseau 192.168.1.0. Vous pouvez choisir toute adresse comprise entre 192.168.1.2 et 192.168.1.254. Excluez les adresses comprises dans la plage qui sera utilisée par le serveur DHCP de votre nouveau routeur (192.168.1.100 à 192.168.1.149). Par exemple, optez pour 192.168.1.250. Notez cette adresse. Vous en aurez besoin ultérieurement pour gérer votre ancien routeur.

4. Dans le champ **Subnet Mask** (masque de sous-réseau) entrez **255.255.255.0** ou, si cela est possible, sélectionnez le masque de sous-réseau dans une liste déroulante.

5. Désactivez le serveur DHCP sur votre ancien routeur. (Étant donné que votre ancien routeur fonctionnera en tant que point d'accès, ce dernier ne doit pas distribuer d'adresses IP. Votre réseau ne doit comprendre qu'un seul serveur DHCP actif, à savoir celui de votre nouveau routeur.)

6. Pour reconfigurer le réseau sans fil sur votre ancien routeur :

   a. Ouvrez la page de configuration du réseau sans fil.

   b. Modifiez le nom du réseau (SSID) de sorte qu'il corresponde à celui de votre nouveau réseau. Une fois que le nom de réseau et les paramètres seront identiques, vous profiterez d'un accès transparent à partir du nouveau et de l'ancien routeur.

   c. Modifiez le mode de sécurité de sorte qu'il corresponde à celui de votre nouveau routeur.

   d. Modifiez la phrase de vérification (parfois appelé clé pré-partagée) de votre ancien routeur de sorte qu'elle corresponde à celle de votre nouveau routeur.

   e. Choisissez un canal sans fil qui ne créera pas de conflit. Certains fabricants proposent une fonction de sélection automatique du canal afin d'éviter les interférences avec les autres réseaux sans fil à proximité. Si votre ancien routeur prend en charge la sélection automatique du canal, activez-la. Sinon, choisissez manuellement le canal de fonctionnement sans fil de votre ancien routeur. La bande de fréquences sans fil 2,4 GHz n'offre que trois canaux sans chevauchement : 1, 6 et 11. Choisissez un canal qui ne chevauchera pas celui de votre nouveau routeur. Par exemple, si votre nouveau routeur fonctionne sur le canal 11, configurez votre ancien routeur sur le canal 1 ou 6.

7. Branchez un câble réseau Ethernet à l'un des ports LAN/Ethernet de votre ancien routeur et au port Ethernet de votre nouveau routeur.

ATTENTION
Ne branchez **pas** le câble au port Internet de votre ancien routeur. Vous risqueriez de ne pas pouvoir configurer le routeur en tant que point d'accès sur le réseau actuel.

Installation de votre nouveau routeur derrière l'ancien

Quel est l'avantage d'installer mon nouveau routeur derrière l'ancien? Vous pouvez avoir besoin d'utiliser votre nouveau routeur derrière un autre dans un certain nombre de cas :

1. Plusieurs locataires partagent la connexion Internet du propriétaire. Dans ce cas, installez votre propre routeur derrière celui du propriétaire afin de créer votre propre réseau privé et d'isoler vos ordinateurs du reste du bâtiment.
2. Vous partagez une connexion Internet au bureau et vous souhaitez contrôler l'accès Internet ou le contenu que consultent vos employés.
3. Vous disposez d'un réseau dont vous voulez étendre la portée ou auquel vous souhaitez ajouter des capacités sans fil.
4. Vous voulez isoler des périphériques réseau plus anciens et moins sécurisés du reste du réseau.

Ajout de votre routeur à un routeur ou une passerelle

Dans la plupart des cas, vous pouvez facilement ajouter votre routeur à un réseau sans fil à l'aide de Cisco Connect. Si vous ne parvenez pas à configurer le routeur supplémentaire à l'aide des instructions ci-dessous, reportez-vous à la section « Partage d'une connexion Internet », page 29, ou « Extension de votre réseau », page 30.

Pour ajouter un routeur à votre réseau sans fil :

1. Insérez le CD de configuration Cisco Connect dans le lecteur de CD/DVD de votre ordinateur, puis suivez les instructions à l'écran.
2. Lorsque l'on vous invite à connecter le port **Internet** de votre routeur au port **LAN/Ethernet** de votre modem, connectez le port **Internet** de votre routeur au port **LAN/Ethernet** de la passerelle ou du routeur existant (en amont).
3. Suivez les instructions à l'écran pour terminer la configuration.

Partage d'une connexion Internet

REMARQUE
Cette procédure est relativement complexe. Vous devez donc disposer de connaissances préalables en réseautage.

Pour ajouter un routeur afin de partager une connexion Internet :

Cette rubrique porte sur les deux premiers cas évoqués précédemment.

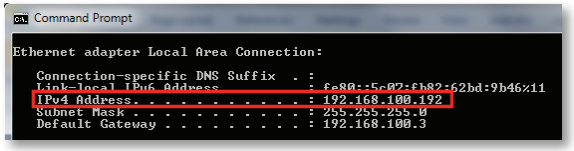
1. Déterminez la plage d'adresses IP de votre réseau en amont (bureau ou bâtiment).

   Pour déterminer la plage d'adresses sur un ordinateur Windows :

   a. Connectez votre ordinateur au routeur de votre réseau en amont.

   b. Cliquez sur **Démarrer**, sur **Exécuter**, tapez **CMD** et cliquez sur **OK**. La fenêtre d'invite de commande s'affiche.

   c. Tapez **ipconfig** et appuyez sur **Entrée**.


Command Prompt
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::5c07:fb82:62bd:9b46%11
IPv4 Address. . . . . : 192.168.100.192
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.100.3

CONSEIL
Bien qu'il existe plusieurs moyens de trouver l'adresse IP de votre ordinateur, cette méthode est très rapide.

   d. Notez l'adresse IP. Dans cet exemple, l'adresse IP est 192.168.100.192.

Pour déterminer la plage d'adresses sur un ordinateur Mac :

   a. Connectez votre ordinateur au routeur de votre réseau en amont.

   b. À partir du *Dock*, cliquez sur **Préférences système**, puis sur **Réseau** et sur **Ethernet** dans la fenêtre à gauche. Une fenêtre d'état du réseau s'affiche.

   c. Notez l'adresse IP. Dans cet exemple, l'adresse IP est 192.168.100.139.

Exemple : Dans les exemples qui précèdent, les adresses IP en amont se situent sur le réseau 192.168.100.0. (Le chiffre « 0 » indique qu'il s'agit de l'ensemble du réseau.) Votre adresse de réseau en amont sera peut-être différente. L'adresse par défaut de votre nouveau routeur Linksys est 192.168.1.1. Lorsque vous installez un routeur derrière un autre, vous devez vous assurer que le réseau local de votre nouveau routeur est différent du réseau du routeur en amont. Dans l'exemple qui précède, le réseau local par défaut de votre routeur Linksys 192.168.1.0 est situé sur un sous-réseau différent du réseau du bureau 192.168.100.0. Vous pourrez donc placer votre routeur Linksys derrière l'autre routeur.

2. À l'aide d'un câble réseau Ethernet, reliez le port LAN/Ethernet de votre réseau en amont au port **Internet** jaune de votre routeur.

ATTENTION
Connectez le réseau en amont au port **Internet** jaune de votre routeur et *non* à l'un des ports Ethernet bleus. Des problèmes d'adressage IP risqueraient de survenir sur le réseau du bureau.

CONSEILS
Dans les réseaux de bureau, vous pouvez généralement effectuer la connexion sur une plaque murale dotée d'un port Ethernet.

Dans le cadre d'une installation résidentielle (où il n'y a pas de ports muraux), utilisez un câble réseau Ethernet pour relier un port LAN du routeur en amont et le port **Internet** de votre routeur Linksys.

3. Ouvrez Cisco Connect sur chaque ordinateur que vous voulez connecter au routeur Linksys. Chaque ordinateur doit être relié par câble ou par liaison sans fil au routeur Linksys. Pour en savoir davantage, reportez-vous à la section « Connexion d'un ordinateur à votre réseau », page 10.

Les ordinateurs connectés au routeur Linksys sont désormais sur le même réseau et sont isolés du réseau en amont. Cependant, le routeur en amont continue de fournir l'accès à Internet (par l'intermédiaire de votre routeur Linksys). Étant donné que deux routeurs sont placés entre votre ordinateur et Internet, le trafic Internet subit deux traductions d'adresses réseau. C'est ce que l'on appelle parfois le *double NAT*.

Vous pouvez aussi utiliser les fonctionnalités intégrées à votre routeur Linksys sur vos ordinateurs, comme le contrôle parental. Si vous avez besoin de contrôler davantage le type de contenu auquel accèdent vos employés ou votre famille, créez un compte auprès d'un site de filtrage Internet tel que **www.opendns.com** ou **www.bsecure.com**. Ensuite, utilisez ce DNS au lieu de celui de votre FAI.

Pour utiliser le DNS d'un fournisseur de filtrage :

Setup (configuration) > Basic Setup (configuration de base)

1. Accédez à l'utilitaire Web (reportez-vous à la section « Ouverture de l'utilitaire Web », page 18).
2. Cliquez sur l'onglet **Setup** (configuration), puis sur la page **Basic Setup** (configuration de base).
3. Remplissez les champs **Static DNS** (DNS statique) à l'aide des informations communiquées par votre fournisseur de filtrage de contenu.

4. Cliquez sur **Save Settings** (enregistrer les paramètres).

Extension de votre réseau

Cette rubrique porte sur les deux derniers cas évoqués précédemment.

REMARQUE
Cette procédure est relativement complexe. Vous devez donc disposer de connaissances préalables en réseautage.

Pour étendre votre réseau ou ajouter des capacités sans fil :

1. Si vous voulez étendre votre réseau, vous pouvez également suivre les instructions qui précèdent. Par exemple, vous souhaiterez peut-être mettre en place un réseau sans fil distinct pour vos enfants, afin de séparer le trafic de leur réseau de celui du réseau sans fil. Vous aurez peut-être aussi besoin d'isoler un réseau d'un autre, de sorte que les partages ne soient pas visibles sur ces réseaux. Dans ce cas, utilisez un câble Ethernet pour relier le port **Internet** du routeur en aval à l'un des ports LAN du routeur en amont. Assurez-vous que les deux routeurs sont associés à des sous-réseaux locaux différents.

   - OU -

   Vous pouvez étendre votre réseau en transformant le routeur en aval en point d'accès. (Reportez-vous à la section « Utilisation d'un routeur en tant que point d'accès », page 26). Lorsque vous utilisez votre routeur en tant que point d'accès, les ordinateurs connectés au point d'accès fonctionnent sur le même sous-réseau IP que tous les autres périphériques connectés au routeur. Cela facilite le partage de fichiers, d'imprimantes et de contenu multimédia.

Exposition d'un périphérique sur Internet

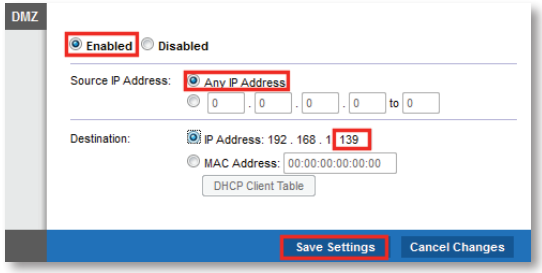
Pourquoi exposer un périphérique sur Internet? Si vous utilisez un serveur Web, un serveur de messagerie ou une caméra Web, vous souhaiterez peut-être l'exposer sur Internet de sorte que tous les utilisateurs puissent y accéder. Votre routeur inclut une fonction de zone publique, ou *DMZ* (Demilitarized Zone). Elle redirige tous les ports entrants présentés sur l'interface WAN vers une adresse IP ou MAC individuelle, hormis ceux qui font l'objet d'un routage spécifique. En général, cette fonction n'est pas utilisée car elle présente des risques de sécurité importants pour le périphérique choisi pour la zone publique. Le périphérique DMZ n'est pas protégé par les pare-feu intégrés, les filtres Internet ou les filtres Web du routeur. Il est donc vulnérable aux attaques des pirates.

Pour « exposer » des périphériques sur Internet, il est préférable d'opter pour le routage de port. Reportez-vous à la section « Configuration du routage de port », page 46.

Pour configurer un périphérique dans la zone publique :

Applications & Gaming (applications et jeux) > DMZ (zone publique)

1. Configurez votre périphérique de sorte qu'il fonctionne sur une adresse IP statique. Consultez la documentation de votre périphérique pour savoir comment définir une adresse IP statique ou utiliser la réservation DHCP (reportez-vous à la section « Configuration du serveur DHCP sur votre routeur », page 20).
2. Accédez à l'utilitaire Web (reportez-vous à la section « Ouverture de l'utilitaire Web », page 18).
3. Cliquez sur l'onglet **Applications & Gaming** (applications et jeux), puis sur la page **DMZ** (zone publique).
4. Sélectionnez **Enabled** (activé).
5. Dans la section *Source IP Address* (adresse IP source), sélectionnez **Any IP Address** (toute adresse IP) afin d'autoriser votre périphérique DMZ à accéder entièrement à Internet. Vous pouvez également sélectionner le bouton **source range** (plage source) pour entrer une plage d'adresses sources autorisées.
6. Dans la section *Destination*, entrez les trois derniers chiffres de l'adresse IP du périphérique qui se trouvera dans la zone publique. Le reste de l'adresse IP est déjà rempli.
7. Cliquez sur **Save Settings** (enregistrer les paramètres) pour appliquer les modifications.



Si vous préférez spécifier l'adresse MAC à 12 chiffres du périphérique à placer en zone publique au lieu de configurer la réservation d'adresses DHCP, procédez comme suit au lieu de suivre l'étape 6 :

a. Cliquez sur **Enabled** (activé).

b. Dans la section *Source IP Address* (adresse IP source), conservez le paramètre par défaut **Any IP Address** (toute adresse IP) afin d'autoriser votre périphérique DMZ à accéder entièrement à Internet. Vous pouvez également sélectionner le bouton **source range** (plage source) pour entrer une plage d'adresses sources autorisées.

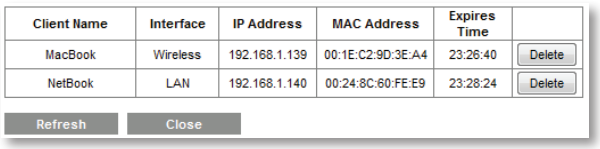
c. Dans la section *Destination*, sélectionnez **MAC Address** (adresse MAC), puis cliquez sur **DHCP Client Table** (table des clients DHCP). Une nouvelle fenêtre s'ouvre et affiche la liste des clients DHCP actuels.

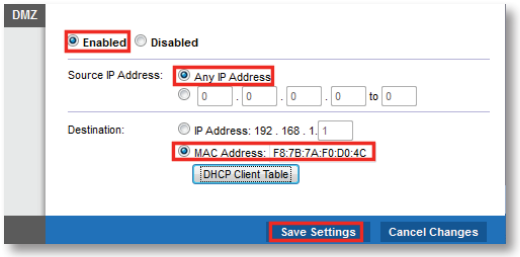
d. Cliquez sur **Select** (sélectionner) à côté du périphérique à placer dans la zone publique. Dans cet exemple, le premier périphérique a été sélectionné. L'adresse MAC correspondante a été copiée dans le champ *MAC Address* (adresse MAC) comme illustré ci-dessous.

e. Cliquez sur **Save Settings** (enregistrer les paramètres) pour appliquer les modifications.

CONSEIL

La table des clients DHCP ne s'affiche que si vous sélectionnez **MAC Address** (adresse MAC).


Client Name
Interface
IP Address
MAC Address
Expires Time
MacBook
Wireless
192.168.1.139
00:1E:C2:9D:3E:A4
23:26:40
Delete
NetBook
LAN
192.168.1.140
00:24:8C:60:FE:E9
23:28:24
Delete
Refresh
Close


DMZ
Enabled
Disabled
Source IP Address:
Any IP Address
0 . 0 . 0 . 0 to 0
Destination:
IP Address: 192 . 168 . 1. 1
MAC Address: F8:7B:7A:F0:D0:4C
DHCP Client Table
Save Settings
Cancel Changes

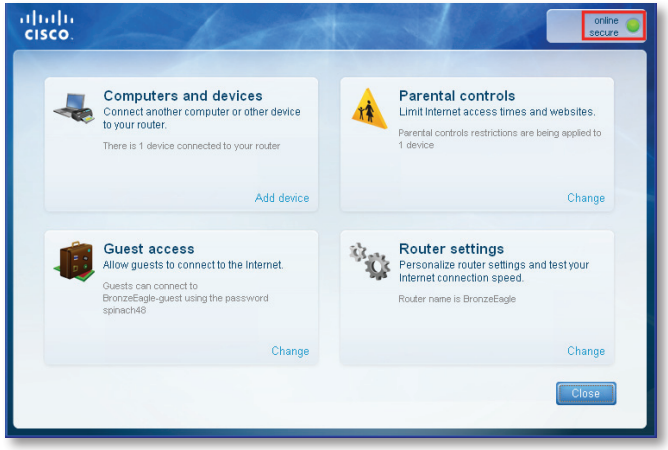
Optimisation de la sécurité

Comment savoir si mon réseau est sécurisé?

Si vous avez configuré votre routeur à l'aide de Cisco Connect, votre réseau est sécurisé. Durant la configuration, Cisco Connect crée un nom pour votre réseau, active la norme de sécurité sans fil WPA/WPA2 et attribue un mot de passe hautement sécurisé à votre réseau sans fil et au compte d'administrateur.

Pour vérifier que votre réseau est sécurisé :

1. Ouvrez Cisco Connect.


cisco
online
secure
Computers and devices
Connect another computer or other device to your router.
There is 1 device connected to your router
Add device
Parental controls
Limit Internet access times and websites.
Parental controls restrictions are being applied to 1 device
Change
Guest access
Allow guests to connect to the Internet.
Guests can connect to BronzeEagle-guest using the password spinach48
Change
Router settings
Personalize router settings and test your Internet connection speed.
Router name is BronzeEagle
Change
Close

2. Vérifiez qu'un point vert apparaît dans le coin supérieur droit de l'écran. Il indique que votre routeur est en ligne et sécurisé. Aucune mesure supplémentaire n'est nécessaire.

Sécurité du réseau après une configuration manuelle

Si vous avez configuré votre routeur manuellement (déconseillé), vous devez également configurer manuellement la sécurité.

Pour définir manuellement le mot de passe du routeur :

Administration > Management (gestion)

1. Accédez à l'utilitaire Web (reportez-vous à la section « Ouverture de l'utilitaire Web », page 18).
2. Cliquez sur l'onglet **Administration** puis sur la page **Management** (gestion).
3. Dans la section *Router Access* (accès au routeur), entrez un mot de passe sécurisé pour le routeur, puis confirmez-le. Votre mot de passe doit au moins comporter au moins huit caractères. Le type de mot de passe sécurisé doit inclure des lettres en majuscules et minuscules, ainsi que des chiffres et des signes de ponctuation.
4. Cliquez sur **Save Settings** (enregistrer les paramètres) au bas de l'écran.

Pour définir manuellement le nom de réseau (SSID) du routeur :

Wireless (sans fil) > Basic Wireless Settings (paramètres de base du réseau sans fil)

1. Accédez à l'utilitaire Web (reportez-vous à la section « Ouverture de l'utilitaire Web », page 18).
2. Cliquez sur l'onglet **Wireless** (sans fil) puis sur la page **Basic Wireless Settings** (paramètres de base du réseau sans fil).
3. Réglez l'option *Configuration View* (vue de configuration) sur **Manual** (manuel).
4. Entrez un nom de réseau dans le champ **Network Name (SSID)** (nom de réseau SSID), puis cliquez sur **Save Settings** (enregistrer les paramètres) au bas de l'écran.

Pour définir manuellement les paramètres de sécurité sans fil de votre routeur :

Wireless (sans fil) > Wireless Security (sécurité du réseau sans fil)

1. Accédez à l'utilitaire Web (reportez-vous à la section « Ouverture de l'utilitaire Web », page 18).
2. Cliquez sur l'onglet **Wireless** (sans fil) puis sur la page **Wireless Security** (sécurité du réseau sans fil).
3. Sélectionnez un type de sécurité dans la liste déroulante **Security Mode** (mode de sécurité). Pour la plupart des réseaux domestiques, nous recommandons **WPA2/WPA Mixed Mode** (mode mixte WPA2/WPA).
4. Entrez une phrase de vérification (ou clé de sécurité) pour votre réseau sans fil dans le champ **Passphrase** (phrase de vérification). Le type de clé de sécurité doit inclure des lettres en majuscules et minuscules, ainsi que des chiffres et des signes de ponctuation.
5. Cliquez sur **Save Settings** (enregistrer les paramètres) au bas de l'écran.

Configuration de la sécurité sans fil à l'aide de la fonction Wi-Fi Protected Setup

Pourquoi utiliser la fonction Wi-Fi Protected Setup? La configuration de l'accès Wi-Fi protégé Wi-Fi Protected Setup[MC] de votre routeur facilite l'ajout de périphériques sur votre réseau sans fil. Si votre réseau comprend des périphériques tels que des imprimantes sans fil qui prennent en charge la fonction Wi-Fi Protected Setup, vous pouvez utiliser cette méthode.

Voyant d'activité Wi-Fi Protected Setup

Le voyant d'alimentation au dos du routeur (ou en haut du modèle E4200) indique l'état de la fonction Wi-Fi Protected Setup lorsque vous connectez des périphériques.

- Lorsque la fonction Wi-Fi Protected Setup connecte un périphérique réseau, le voyant clignote lentement.
- En cas d'erreur, le voyant clignote rapidement pendant deux minutes. Attendez que le voyant cesse de clignoter, puis réessayez.
- Lorsque la fonction Wi-Fi Protected Setup a terminé de connecter un périphérique, le voyant reste allumé.
- Attendez que le voyant reste allumé en permanence avant de commencer la deuxième session Wi-Fi Protected Setup.

Connectez les périphériques réseau en suivant l'une des trois méthodes ci-dessous.

REMARQUE
La configuration Wi-Fi Protected Setup s'effectue un périphérique client à la fois. Répétez la procédure pour chaque périphérique prenant en charge la fonction Wi-Fi Protected Setup.

Connexion d'un périphérique à l'aide du bouton Wi-Fi Protected Setup

Suivez cette méthode si votre périphérique est doté d'un bouton Wi-Fi Protected Setup ou si le périphérique vous invite à appuyer sur le bouton Wi-Fi Protected Setup de votre routeur.

Pour connecter un périphérique à l'aide du bouton Wi-Fi Protected Setup :

Wireless (sans fil) > Basic Wireless Settings (paramètres de base du réseau sans fil)

1. Appuyez sur le bouton **Wi-Fi Protected Setup** du périphérique réseau que vous connectez.
2. Appuyez sur le bouton **Wi-Fi Protected Setup** au dos du routeur.

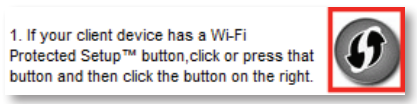
   - OU -

   a. Accédez à l'utilitaire Web (reportez-vous à la section « Ouverture de l'utilitaire Web », page 18).

   b. Cliquez sur l'onglet **Wireless** (sans fil) puis sur la page **Basic Wireless Settings** (paramètres de base du réseau sans fil).

   c. Cliquez sur **Wi-Fi Protected Setup**.

   d. Cliquez sur le bouton **WiFi Protected Setup** dans la page *Wi-Fi Protected Setup* du routeur.


1. If your client device has a Wi-Fi Protected Setup™ button,click or press that button and then click the button on the right.

   e. Une fois le périphérique configuré, cliquez sur **OK**.

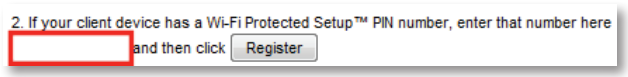
Connexion d'un périphérique à l'aide de son NIP Wi-Fi Protected Setup

Suivez cette méthode si votre périphérique dispose d'un numéro d'identification personnel, ou *NIP* Wi-Fi Protected Setup.

Pour connecter un périphérique à l'aide de son NIP Wi-Fi Protected Setup :

Wireless (sans fil) > Basic Wireless Settings (paramètres de base du réseau sans fil)

1. Accédez à l'utilitaire Web (reportez-vous à la section « Ouverture de l'utilitaire Web », page 18).
2. Cliquez sur l'onglet **Wireless** (sans fil) puis sur la page **Basic Wireless Settings** (paramètres de base du réseau sans fil).
3. Cliquez sur **Wi-Fi Protected Setup**.
4. Entrez le NIP du périphérique dans le champ **PIN** (NIP) à l'écran *Wi-Fi Protected Setup* du routeur, puis cliquez sur **Register** (enregistrer).



5. Une fois le périphérique connecté, cliquez sur **OK**.

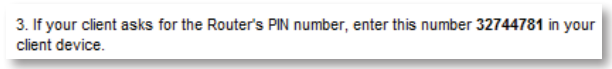
Connexion d'un périphérique à l'aide du NIP Wi-Fi Protected Setup du routeur

Suivez cette méthode si votre périphérique client demande le NIP du routeur.

Pour connecter un périphérique à l'aide de son NIP Wi-Fi Protected Setup :

Wireless (sans fil) > Basic Wireless Settings (paramètres de base du réseau sans fil)

1. Accédez à l'utilitaire Web (reportez-vous à la section « Ouverture de l'utilitaire Web », page 18).
2. Cliquez sur l'onglet **Wireless** (sans fil) puis sur la page **Basic Wireless Settings** (paramètres de base du réseau sans fil).
3. Cliquez sur **Wi-Fi Protected Setup**.
4. Sur le périphérique client, entrez le NIP indiqué à l'écran *Wi-Fi Protected Setup* du routeur. Le NIP est indiqué au bas du routeur. Dans l'exemple ci-dessous, le NIP du routeur est 32744781.



5. Suivez les instructions du périphérique pour effectuer la configuration.

Connexion manuelle d'un périphérique

Si certains de vos périphériques ne prennent pas en charge la fonction Wi-Fi Protected Setup, notez les paramètres sans fil indiqués à l'écran *Basic Wireless Settings* (paramètres de base du réseau sans fil), puis configurez manuellement ces périphériques.

Pour chaque réseau sans fil, vous trouverez le nom de réseau sans fil (SSID), le mode de sécurité et la phrase de vérification au bas de la page.

Contrôle de l'accès à votre réseau sans fil

Dans quel cas est-il nécessaire de contrôler l'accès au réseau sans fil? Si vous avez utilisé Cisco Connect pour configurer votre routeur, votre réseau sans fil est déjà sécurisé. Par défaut, Cisco Connect active la norme de sécurité *WPA* (Wi-Fi Protected Access) à l'aide du mode mixte WPA2/WPA. Cisco Connect configure votre réseau à l'aide d'un mot de passe complexe de 10 caractères qu'il est presque impossible de pirater. Si vous avez configuré votre réseau sans fil manuellement et que vous n'avez pas activé la sécurité sans fil, votre réseau sera ouvert à presque tous les périphériques Wi-Fi à proximité.

Qu'est-ce que le filtrage des adresses MAC? Le meilleur moyen de sécuriser votre réseau sans fil est d'utiliser Cisco Connect. Le logiciel procédera automatiquement à sa configuration et à sa sécurisation. Cependant, si vous choisissez ne pas utiliser les fonctionnalités de sécurité intégrées de votre routeur, vous pouvez toujours contrôler l'accès à votre réseau sans fil à l'aide du filtrage des adresses MAC.

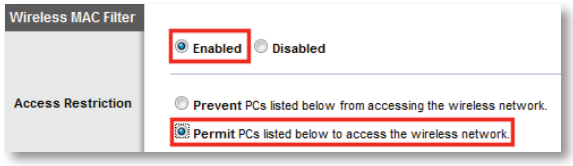
Chaque périphérique réseau est associé à une adresse *MAC* (Media Access Control) unique de 12 chiffres. Le filtrage des adresses MAC permet de restreindre l'accès au réseau aux adresses MAC connues. Vous pouvez également exclure des adresses MAC ou leur refuser l'accès à votre réseau sans fil.

Exemple : Chaque configuration de filtrage des adresses MAC est unique. La procédure qui suit donne donc un exemple de configuration de filtrage simplifié, permettant d'autoriser un périphérique sans fil à accéder au réseau.

Pour configurer le filtrage des adresses MAC afin d'autoriser un périphérique sans fil à accéder à votre réseau :

Wireless (sans fil) > Wireless MAC Filter (filtrage des adresses MAC sans fil)

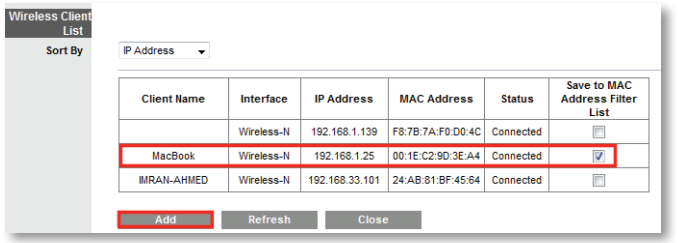
1. Accédez à l'utilitaire Web (reportez-vous à la section « Ouverture de l'utilitaire Web », page 18).
2. Cliquez sur l'onglet **Wireless** (sans fil) puis sur la page **Wireless MAC Filter** (filtrage des adresses MAC sans fil).
3. Cliquez sur **Enabled** (activé).
4. Sélectionnez **Permit** (autoriser).


Wireless MAC Filter
Enabled
Disabled
Access Restriction
Prevent PCs listed below from accessing the wireless network.
Permit PCs listed below to access the wireless network.

CONSEIL

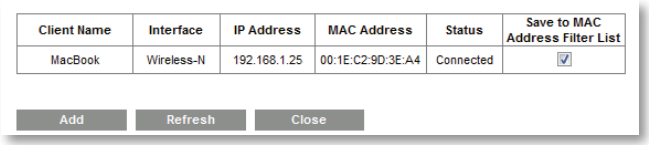
Le filtrage des adresses MAC peut également servir à refuser l'accès au réseau à certains ordinateurs. Pour ce faire, sélectionnez **Prevent** (bloquer). Il est cependant plus simple de n'autoriser que certains périphériques connus à accéder au réseau plutôt que d'exclure des périphériques inconnus.

5. Cliquez sur **Wireless Client List** (liste de périphériques clients sans fil). Une nouvelle fenêtre s'ouvre et affiche la liste des périphériques actuellement connectés. Dans l'exemple ci-après, seul le MacBook est autorisé à se connecter au réseau. Cependant, deux autres périphériques sont également connectés au réseau.



6. À côté du périphérique, sélectionnez **Save to MAC Address Filter List** (enregistrer dans la liste de filtrage d'adresses MAC), puis cliquez sur **Add** (ajouter). La liste se met à jour pour inclure l'adresse MAC du périphérique que vous venez d'ajouter.

7. Cliquez sur **Save Settings** (enregistrer les paramètres) au bas de la page.
8. Cliquez de nouveau sur **Wireless Client List** (liste de périphériques clients sans fil) pour afficher la liste à jour des périphériques. Seul le périphérique sélectionné demeure sur le réseau.



Optimisation de la sécurité à l'aide du pare-feu intégré

Pourquoi modifier mes paramètres de sécurité? Par défaut, les paramètres de pare-feu de votre routeur ont été optimisés pour la plupart des environnements domestiques. Aucune modification n'est donc nécessaire. Le pare-feu *SPI* (Stateful Packet Inspection) est activé par défaut. Les requêtes Internet anonymes et IDENT sont également filtrées par défaut. Tous les filtres Web sont désactivés afin d'éviter les problèmes avec les sites qui utilisent des contrôles ActiveX, Java ou des cookies.

Pour modifier les paramètres de votre pare-feu :

Security (sécurité) ->Firewall (pare-feu)

1. Accédez à l'utilitaire Web (reportez-vous à la section « Ouverture de l'utilitaire Web », page 18).
2. Cliquez sur l'onglet **Security** (sécurité), puis sur la page **Firewall** (pare-feu).
3. Sélectionnez les paramètres que vous souhaitez modifier.

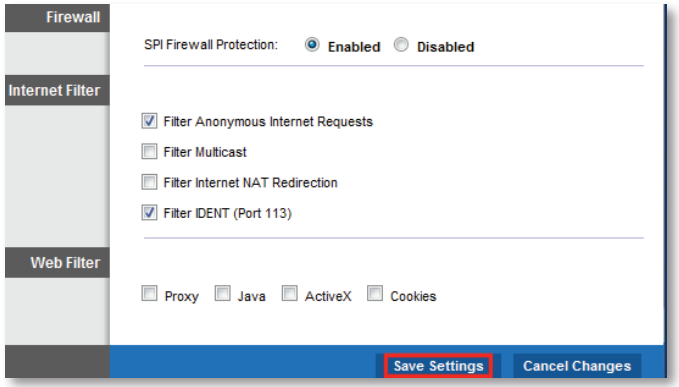
CONSEIL
Pour voir la description des filtres, cliquez sur **Help** à droite de l'écran. Vous trouverez ci-dessous des descriptions plus exhaustives.

- **SPI Firewall Protection** (protection par pare-feu SPI) : Protège votre réseau local des menaces sur Internet. Cette option est activée par défaut.

ATTENTION
Laissez cette option activée afin de mieux protéger votre réseau.

- **Filter Anonymous Internet Requests** (filtrer les requêtes Internet anonymes) : Bloque les requêtes Internet provenant de sources inconnues, telles que les requêtes ping. Cette option est activée par défaut.
- **Filter Multicast** (filtre multidiffusion) : La multidiffusion permet l'envoi simultané d'une même transmission à plusieurs destinataires de votre réseau local. Choisissez cette option pour bloquer la multidiffusion. Cette option est désactivée par défaut.
- **Filter Internet NAT Redirection** (filtrer la redirection NAT Internet) : Ce filtre interdit à un ordinateur local d'utiliser une URL ou une adresse IP Internet pour accéder au serveur local. Sélectionnez cette fonction pour activer le filtre. Cette option est désactivée par défaut.
- **Filter IDENT (Port 113)** (filtrer IDENT, port 113) : Ce filtre évite l'analyse du port 113 par des périphériques depuis Internet. Cette option est activée par défaut.
- **Proxy** : Ce filtre bloque l'utilisation des serveurs proxy Internet. Sélectionnez cette option pour refuser les requêtes proxy. L'accès par proxy est autorisé par défaut.
- **Java** : Ce filtre bloque Java. Vous risquez de ne pas avoir accès au contenu Java des sites Web. Sélectionnez cette option pour refuser les requêtes Java. Le contenu Java est autorisé par défaut.
- **ActiveX** : Ce filtre bloque ActiveX. Vous risquez de ne pas avoir accès au contenu ActiveX des sites Web. Sélectionnez cette option pour refuser les requêtes ActiveX. Le contenu ActiveX est autorisé par défaut.
- **Cookies** : Ce filtre bloque les cookies (données stockées sur votre ordinateur et utilisées par des sites Web que vous visitez). Sélectionnez cette option pour refuser les demandes de cookies. L'utilisation des cookies est autorisée par défaut.

4. Cliquez sur **Save Settings** (enregistrer les paramètres) pour appliquer les modifications.



Utilisation d'un lecteur externe

Configuration du stockage

Dans quels cas est-il nécessaire de configurer le stockage? Lorsque vous connectez un périphérique de stockage à votre routeur, l'intégralité de son contenu est par défaut accessible en lecture et en écriture à tous les utilisateurs de votre réseau local (aucune information de connexion n'est requise). Cependant, vous pouvez également créer des dossiers partagés configurés de sorte que seuls certains groupes y aient accès.

Pour contrôler l'accès au lecteur USB connecté à votre routeur, vous devez effectuer les deux opérations suivantes :

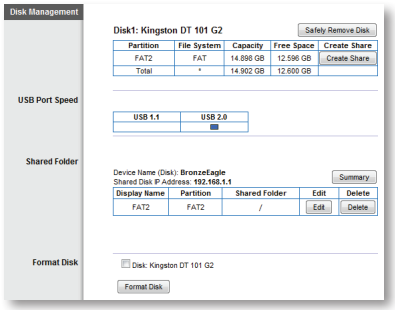
1. Créer un ou plusieurs dossiers partagés (reportez-vous à la section « Création de dossiers partagés » qui suit)
2. Gérer l'accès des groupes et des utilisateurs aux dossiers partagés (reportez-vous à la section « Partage de dossiers et établissement de droits d'accès », page 43)

Création de dossiers partagés

Pour créer un dossier partagé :

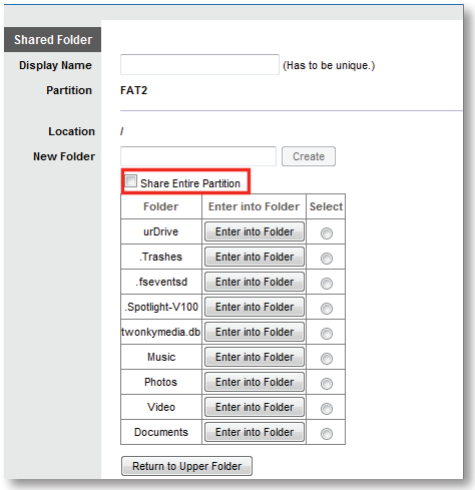
Storage (stockage) > Disk (disque)

1. Accédez à l'utilitaire Web (reportez-vous à la section « Ouverture de l'utilitaire Web », page 18).
2. Cliquez sur l'onglet **Storage** (stockage) puis sur la page **Disk** (disque).



3. Cliquez sur **Create Share** (créer un partage) à côté de la partition à partager. L'écran *Shared Folder* (dossier partagé) s'ouvre.

4. Si vous voulez partager l'intégralité de la partition, sélectionnez **Share Entire Partition** (partager toute la partition), puis cliquez sur **Save Settings** (enregistrer les paramètres) au bas de l'écran.



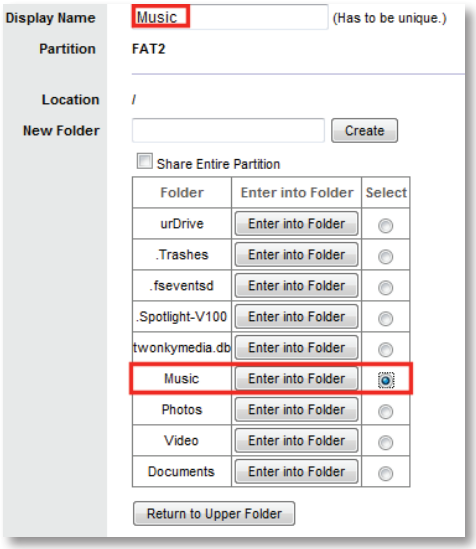
– OU –

Si vous voulez partager un seul dossier :

a. Entrez un nom unique dans le champ **Display Name** (nom d'affichage).

b. Cliquez sur **Select** (sélectionner) à côté du nom du dossier à partager.
   - Pour ouvrir un sous-dossier, cliquez sur **Enter into Folder** (ouvrir le dossier).
   - Pour revenir au dossier précédent, cliquez sur **Return to Upper Folder** (revenir au dossier parent).
   - Pour créer un nouveau dossier, tapez son nom dans le champ **New Folder** (nouveau dossier), puis cliquez sur **Create** (créer).

c. Cliquez sur **Save Settings** (enregistrer les paramètres) au bas de l'écran, puis suivez de nouveau les étapes précédentes pour chaque nouveau dossier à ajouter.



Gestion de l'accès des groupes et utilisateurs aux dossiers partagés

Pour gérer l'accès aux dossiers partagés, désactivez l'option Anonymous Disk Access (accès au disque anonyme), puis créez des groupes et comptes d'utilisateur sur votre routeur. Les comptes d'utilisateur conditionnent l'accès au routeur, tandis que les groupes conditionnent l'accès aux dossiers partagés.

1. Désactivez l'option Anonymous Disk Access (accès au disque anonyme). Reportez-vous à la section « Désactivation de l'accès au disque anonyme », page 40.
2. Créez un groupe auquel vous attribuerez des droits d'accès au dossier partagé.
3. Créez des utilisateurs que vous inclurez dans le groupe.
4. Ajoutez le groupe au dossier partagé dont vous souhaitez contrôler l'accès.

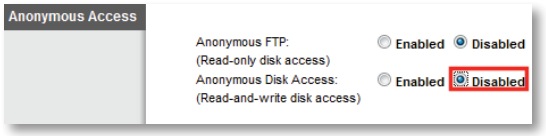
Désactivation de l'accès au disque anonyme

Par défaut, l'accès en lecture et en écriture au disque ne requiert aucun mot de passe. Avant de pouvoir gérer l'accès des groupes et des utilisateurs aux dossiers partagés, vous devez désactiver l'accès au disque anonyme.

Pour désactiver l'accès au disque anonyme

Storage (stockage) > Administration

1. Accédez à l'utilitaire Web (reportez-vous à la section « Ouverture de l'utilitaire Web », page 18).
2. Cliquez sur l'onglet **Storage** (stockage) puis sur la page **Administration**.
3. Réglez l'option *Anonymous Disk Access* (accès au disque anonyme) sur **Disabled** (désactivé).



4. Cliquez sur **Save Settings** (enregistrer les paramètres) au bas de l'écran.

Création d'un groupe

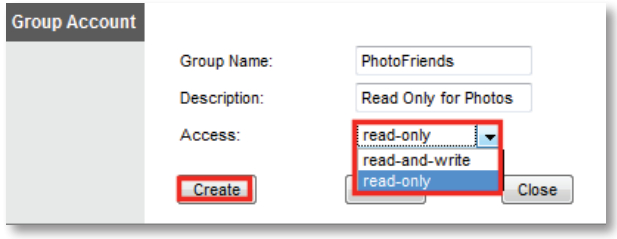
Par défaut, le groupe d'administration (Admin) dispose de droits de lecture et d'écriture pour tous les dossiers partagés. Par défaut, le groupe d'invités (Guest) dispose de droits de lecture seule et n'a accès à aucun des dossiers partagés.

IMPORTANT
Plusieurs groupes peuvent avoir accès à un dossier partagé, mais chaque utilisateur ne peut être membre que d'un seul groupe.

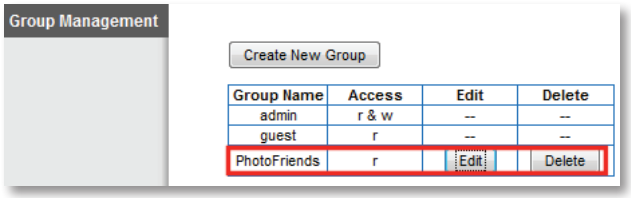
Pour créer un groupe :

Storage (stockage) > Administration

1. Accédez à l'utilitaire Web (reportez-vous à la section « Ouverture de l'utilitaire Web », page 18).
2. Cliquez sur l'onglet **Storage** (stockage) puis sur la page **Administration**.
3. Sous *Group Management* (gestion des groupes), cliquez sur **Create New Group** (créer un groupe).



4. Remplissez les champs **Group Name** (nom du groupe) et **Description**.
5. Dans la liste déroulante **Access** (accès), sélectionnez **read-only** (lecture seule) pour accorder des droits en lecture seule au groupe ou **read-and-write** (lecture/écriture) pour accorder des droits en lecture/écriture.
6. Cliquez sur **Create** (créer). Une fois le groupe créé, les droits d'accès associés s'affichent dans la colonne *Access* (accès).
7. Pour modifier le nom d'un groupe ou ses droits d'accès, cliquez sur **Edit** (modifier) à côté du nom du groupe.
8. Pour supprimer un groupe, cliquez sur **Delete** (supprimer) à côté du nom du groupe.



Création d'un nouvel utilisateur

Deux comptes d'utilisateur sont préconfigurés sur le routeur : *Admin* (administration) et *Guest* (invité). Le mot de passe de l'utilisateur *Admin* est le même que celui permettant d'accéder au routeur. Par défaut, l'utilisateur *Admin* (administration) est membre du groupe *Admin (administration)*, et l'utilisateur *Guest* (invité) est membre du groupe *Guest* (invité). Afin de simplifier la gestion, vous pouvez créer des comptes d'utilisateur sur votre routeur en utilisant les mêmes noms d'utilisateur et mots de passe que ceux du système d'exploitation de votre ordinateur.

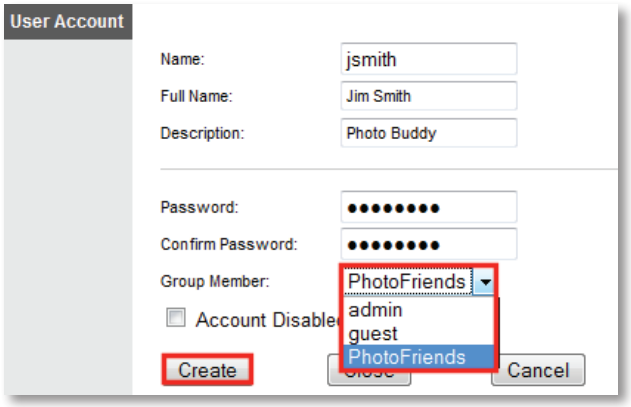
REMARQUE
Chaque utilisateur ne peut être membre que d'un seul groupe.

Pour créer un nouvel utilisateur :

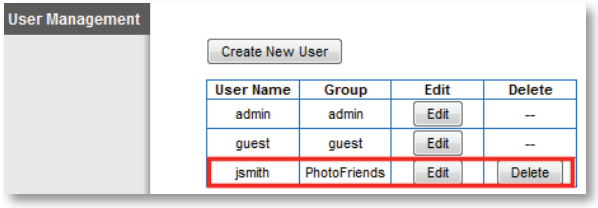
Storage (stockage) > Administration

1. Accédez à l'utilitaire Web (reportez-vous à la section « Ouverture de l'utilitaire Web », page 18).
2. Cliquez sur l'onglet **Storage** (stockage) puis sur la page **Administration**.
3. Sous *User Management* (gestion des utilisateurs), cliquez sur **Create New User** (créer un utilisateur).

4. Remplissez les champs **Name** (nom), **Full Name** (nom complet) et **Description**.
5. Entrez un mot de passe et confirmez-le.
6. Dans la liste déroulante **Group Member** (membre du groupe), sélectionnez le groupe dont fera partie l'utilisateur et cliquez sur **Create** (créer). Le nouvel utilisateur s'affiche dans la liste des utilisateurs.



7. Pour modifier un nom d'utilisateur, sa description ou son groupe, ou pour désactiver temporairement un compte, cliquez sur **Edit** (modifier).



8. Pour supprimer l'utilisateur, cliquez sur **Delete** (supprimer).

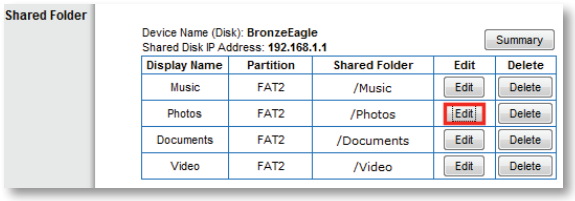
Accès d'un groupe à un dossier partagé

Pour autoriser un groupe à accéder à un dossier partagé

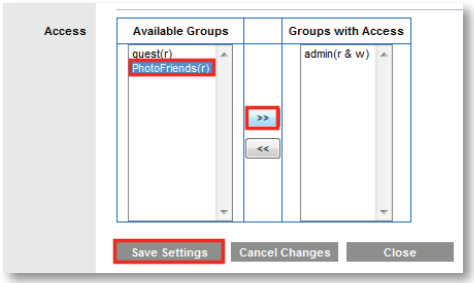
Storage (stockage) > Disk (disque)

1. Accédez à l'utilitaire Web (reportez-vous à la section « Ouverture de l'utilitaire Web », page 18).
2. Assurez-vous que l'option *Anonymous Disk Access* (accès au disque anonyme) est désactivée. (Reportez-vous à la section « Désactivation de l'accès au disque anonyme », page 40.)

3. Cliquez sur l'onglet **Storage** (stockage) puis sur la page **Disk** (disque).
4. Dans la zone *Shared Folder* (dossier partagé), cliquez sur **Edit** (modifier) à côté du dossier partagé auquel le groupe aura accès.



5. Pour autoriser un groupe à accéder au dossier partagé, cliquez sur son nom dans la colonne *Available Groups* (groupes disponibles), puis cliquez sur **>>** pour déplacer le groupe vers la colonne *Groups with Access* (groupes avec accès).
6. Pour interdire à un groupe d'accéder au dossier partagé, sélectionnez son nom dans la colonne *Groups with Access* (groupes avec accès), puis cliquez sur **<<** pour déplacer le groupe vers la colonne *Available Groups* (groupes disponibles).



7. Cliquez sur **Save Settings** (enregistrer les paramètres) pour appliquer les modifications.

Configuration du stockage de votre routeur pour l'accès à distance

Dans quel cas est-il nécessaire de configurer l'accès à distance au stockage de votre routeur? En configurant l'accès à distance au stockage de votre routeur, vous pouvez accéder à vos fichiers à partir de n'importe quelle connexion Internet. Pour ce faire, vous devez activer le serveur FTP (File Transfer Protocol) intégré à votre routeur. Une fois votre routeur configuré, vous pourrez accéder aux fichiers où que vous soyez, par l'intermédiaire d'un navigateur Web ou d'un logiciel de FTP.

Pour configurer votre routeur pour l'accès aux fichiers à distance, vous devez :

1. configurer le serveur FTP;
2. sélectionner les dossiers (ou l'ensemble du lecteur) pour les partager et définir des droits d'accès.

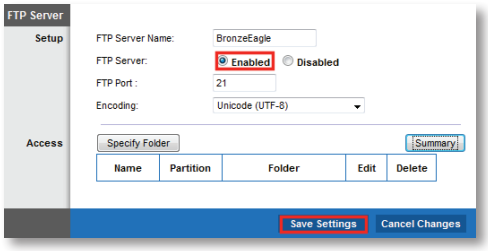
Configuration du serveur FTP

Pour configurer le serveur FTP :

Storage (stockage) > FTP Server (serveur FTP)

1. Accédez à l'utilitaire Web (reportez-vous à la section « Ouverture de l'utilitaire Web », page 18).
2. Cliquez sur l'onglet **Storage** (stockage) puis sur la page **FTP Server** (serveur FTP).

3. Paramétrez l'option *FTP Server* (serveur FTP) sur **Enabled** (activé).



CONSEIL

Si vous avez configuré votre routeur à l'aide de Cisco Connect, le champ FTP Server Name (nom de serveur FTP) comporte déjà le nom de votre réseau sans fil. Si vous avez configuré votre routeur manuellement, vous verrez le nom par défaut Cisco suivi des cinq derniers chiffres du numéro de série de votre routeur.

4. Vous pouvez également :
   - Modifier l'option **FTP Port** (port FTP) du serveur FTP (**21** par défaut).
   - Modifier l'option **Encoding** (encodage), c'est-à-dire le jeu de caractères utilisé pour le transfert des fichiers dans d'autres langues. Le routeur prend en charge :
     - Unicode (UTF-8) (par défaut)
     - Chinois simplifié (GB18030)
     - Vietnamien (CP1258)
     - ISO 8859_1.

CONSEIL

Pour voir la description des champs, cliquez sur **Help** (aide) à droite de l'écran.

5. Pour appliquer les modifications, cliquez sur **Save Settings** (enregistrer les paramètres).

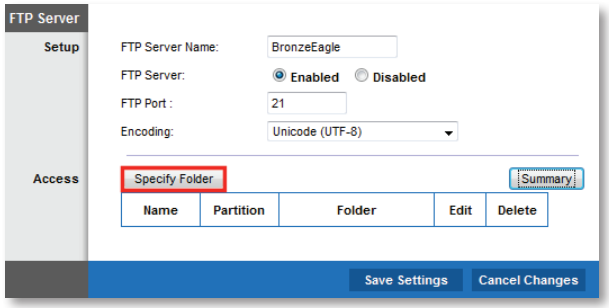
Partage de dossiers et établissement de droits d'accès

Vous pouvez choisir les dossiers à partager. Il est également possible de sélectionner les utilisateurs autorisés à accéder aux dossiers. Pour en savoir plus sur la gestion des droits d'accès, reportez-vous à la section « Configuration du stockage », page 38.

Pour configurer le FTP et contrôler l'accès aux dossiers :

Storage (stockage) > FTP Server (serveur FTP)

1. À l'onglet *Storage* (stockage) de la page *FTP Server* (serveur FTP), cliquez sur **Specify Folder** (spécifier le dossier).



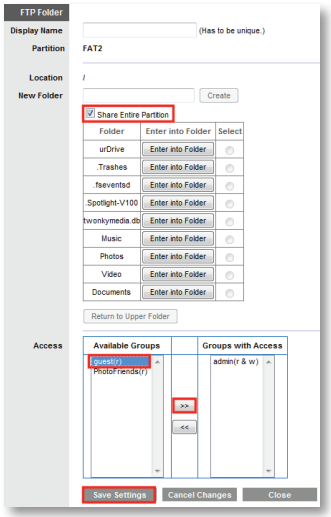
L'écran *FTP Folder* (dossier FTP) s'ouvre dans une nouvelle fenêtre.

2. Dans le champ **Display Name** (nom d'affichage), entrez un nom unique pour le dossier FTP. Les noms peuvent compter jusqu'à 15 caractères alphanumériques (lettres de A à Z et chiffres de 0 à 9).
3. Pour partager l'intégralité du lecteur, cliquez sur **Share Entire Partition** (partager toute la partition).

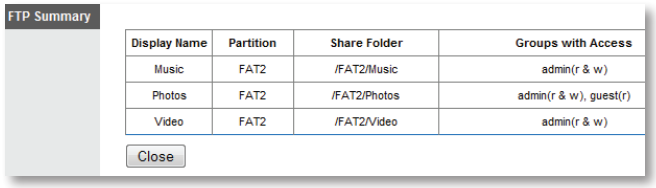
   - OU -

   Pour partager uniquement certains dossiers :
   - Cliquez sur **Select** (sélectionner) à côté du dossier à partager.
   - Pour revenir au dossier précédent, cliquez sur **Return to Upper Folder** (revenir au dossier parent).
   - Pour afficher et sélectionner des dossiers contenus dans un autre, cliquez sur **Enter into Folder** (ouvrir le dossier) à côté du nom du dossier.
4. Pour créer un dossier, entrez un nom de dossier unique dans la zone **New Folder** (nouveau dossier), puis cliquez sur **Create** (créer).

5. Pour modifier les droits d'accès d'un groupe, sélectionnez ce dernier dans la colonne *Available Groups* (groupes disponibles) ou *Groups with Access* (groupes avec accès), puis cliquez sur >> ou << pour déplacer le groupe dans l'autre colonne.
6. Pour appliquer vos modifications et activer l'accès FTP, cliquez sur **Save Settings** (enregistrer les paramètres).



7. Pour appliquer les modifications et créer le dossier partagé accessible par FTP, cliquez sur **Save Settings** (enregistrer les paramètres). La page *FTP Server* (serveur FTP) s'affiche de nouveau, avec le sommaire des dossiers partagés.
8. Pour modifier les paramètres d'un dossier partagé :
   - Pour modifier le nom d'un dossier FTP ou les droits d'accès d'un groupe, cliquez sur **Edit** (modifier).
   - Pour supprimer un dossier FTP, cliquez sur **Delete** (supprimer).
   - Pour voir un sommaire détaillé des dossiers FTP, cliquez sur **Summary** (sommaire). Une nouvelle fenêtre s'ouvre et affiche les renseignements suivants : *Display Name* (nom d'affichage), *Partition*, *Share Folder* (dossier partagé) et *Groups with Access* (groupes avec accès). Cliquez sur **Close** (fermer) pour fermer la fenêtre.



Accès à des fichiers à distance

Pour accéder à des fichiers à distance, vous devez tout d'abord connecter un lecteur USB à votre routeur et configurer l'accès distant au stockage. Pour obtenir des instructions, reportez-vous à la section « Configuration du stockage de votre routeur pour l'accès à distance », page 42. Vous pourrez ensuite accéder aux fichiers depuis Internet, où que vous soyez.

Pour accéder à des fichiers à distance :

1. Assurez-vous que votre routeur est configuré pour le partage de fichiers. Pour en savoir davantage, reportez-vous à la section « Configuration du stockage de votre routeur pour l'accès à distance », page 42.
2. Assurez-vous que des comptes d'utilisateur sont configurés sur votre routeur et notez le nom d'utilisateur et le mot de passe requis pour l'accès au stockage du routeur. Si l'option Anonymous FTP (FTP anonyme) est activée (déconseillé), vous n'aurez pas besoin de nom d'utilisateur ni de mot de passe. Pour en savoir davantage, reportez-vous à la section « Configuration du stockage », page 38.

3. Notez l'adresse IP de votre routeur. Pour connaître l'adresse IP de votre routeur, ouvrez l'utilitaire Web et cliquez sur l'onglet **Status** (état). Cliquez ensuite sur la page **Router** (routeur) et notez les numéros figurant dans le champ *Internet IP Address* (adresse IP Internet).

   – OU –

   Si vous disposez d'un service *DDNS* (Dynamic Domain Name Service), notez le nom de domaine enregistré pour votre routeur. Pour en savoir davantage, reportez-vous à la section « Localisation de votre réseau sur Internet », page 21.

4. Vous pouvez effectuer les opérations suivantes à distance, à partir de toute connexion Internet :

   - Utiliser un logiciel client FTP (File Transfer Protocol) pour vous connecter à votre routeur. Vous aurez besoin d'entrer l'adresse IP de votre routeur. Si l'accès à votre routeur requiert un nom d'utilisateur et un mot de passe, vous devrez les entrer. Pour en savoir plus sur l'utilisation du logiciel client FTP, reportez-vous à la documentation ou à l'aide du logiciel.

     – OU –

   - Entrez l'adresse IP du routeur dans le champ d'adresse d'un navigateur Web, appuyez sur **Entrée**, puis entrez votre nom d'utilisateur et votre mot de passe.

     Le logiciel FTP et le navigateur Web affichent le contenu du FTP de différentes façons. En général, vous pouvez procéder comme suit pour naviguer dans les dossiers FTP :

     - Cliquez sur le nom d'un dossier pour l'ouvrir.
     - Cliquez sur le double point (..) ou **Répertoire de plus haut niveau** pour ouvrir un dossier parent.
     - Cliquez ou double-cliquez avec le bouton droit de la souris sur un fichier pour l'ouvrir ou le télécharger.
     - Pour charger un fichier, faites-le glisser d'une autre fenêtre et déposez-le dans la fenêtre FTP. (Pour charger d'un fichier, votre compte d'utilisateur doit disposer d'un accès en écriture.)

Routage et déclenchement de port

Configuration du routage de port

Dans quels cas utiliser le routage de port? Le routage de port redirige le trafic entrant d'Internet depuis un ou plusieurs ports définis vers un périphérique ou port spécifique de votre réseau local. Vous pouvez définir le routage de port depuis :

- un port unique (reportez-vous à la section « Configuration du routage de port unique » ci-dessous);
- plusieurs ports (reportez-vous à la section « Configuration du routage pour plusieurs ports », page 47);
- une plage de ports (reportez-vous à la section « Configuration du routage d'une plage de ports », page 47).

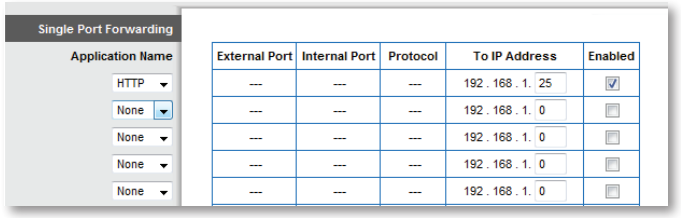
Configuration du routage de port unique

Dans quels cas utiliser le routage de port unique? Le routage de port unique redirige le trafic entrant d'Internet depuis un port défini vers un seul périphérique de votre réseau local. Par exemple, le routage de port unique peut permettre de rediriger les requêtes Web entrantes, en général du port 80, vers un serveur Web.

Pour configurer le routage de port unique :

Applications & Gaming (applications et jeux) > Single Port Forwarding (routage de port unique)

1. Suivez les instructions de configuration de votre périphérique avec une adresse IP statique ou utilisez la réservation DHCP pour lui attribuer une adresse permanente (reportez-vous à la section « Configuration du serveur DHCP sur votre routeur », page 20).
2. Accédez à l'utilitaire Web (reportez-vous à la section « Ouverture de l'utilitaire Web », page 18).
3. Cliquez sur l'onglet **Applications & Gaming** (applications et jeux), puis sur la page **Single Port Forwarding** (routage de port unique).



4. Sélectionnez le type d'application dans la liste déroulante **Application Name** (nom de l'application). **HTTP** fait partie des types les plus courants. Consultez néanmoins la documentation de votre périphérique pour connaître le type recommandé.
5. Dans le champ **To IP Address** (vers adresse IP), entrez les trois derniers chiffres de l'adresse IP réservée pour l'ordinateur vers lequel vous voulez rediriger le trafic Internet. Le reste de l'adresse IP est déjà rempli.
6. Sélectionnez **Enabled** (activé) à côté du champ *IP Address* (adresse IP).
7. Cliquez sur **Save Changes** (enregistrer les modifications) au bas de l'écran.

CONSEIL
Pour les autres périphériques qui ne figurent pas dans la liste déroulante Application Name (nom de l'application), reportez-vous à la documentation du périphérique pour en savoir plus sur les ports et protocoles.

Configuration du routage pour plusieurs ports

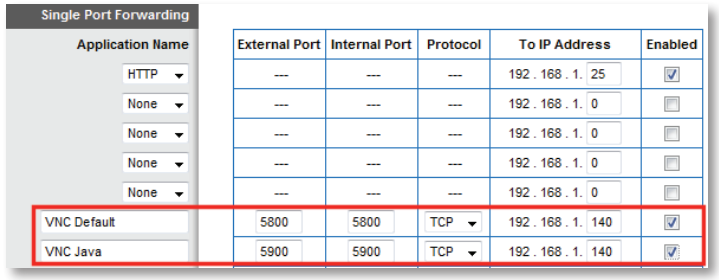
Dans quels cas utiliser le routage pour plusieurs ports? Le routage de port redirige le trafic entrant d'Internet depuis un port défini vers un seul périphérique de votre réseau local. Contrairement à une caméra Web qui nécessite généralement le routage d'un port unique, certaines applications requièrent le routage de plusieurs ports. C'est notamment le cas des applications telles que le logiciel *VNC* (Virtual Network Computing), qui permet d'utiliser un ordinateur à distance depuis n'importe où sur Internet. Pour rediriger plusieurs ports, créez des entrées supplémentaires afin d'assurer le routage de ports supplémentaires vers la même adresse IP.

Exemple : Vous souhaitez configurer votre ordinateur de sorte à pouvoir y accéder à distance au moyen du logiciel VNC. Par défaut, VNC utilise les ports TCP 5800 et 5900.

Pour configurer le routage de port unique pour plusieurs ports :

Applications & Gaming (applications et jeux) > Single Port Forwarding (routage de port unique)

1. Assurez-vous que le logiciel que vous souhaitez utiliser a été installé sur un ordinateur du réseau.
2. Accédez à l'utilitaire Web (reportez-vous à la section « Ouverture de l'utilitaire Web », page 18).
3. Configurez la réservation DHCP pour l'adresse IP de l'ordinateur sur lequel vous avez installé le logiciel. (Reportez-vous à la section « Configuration du serveur DHCP sur votre routeur », page 20).
4. Cliquez sur l'onglet **Applications & Gaming** (applications et jeux), puis sur la page **Single Port Forwarding** (routage de port unique).
5. Pour chaque entrée, entrez un nom descriptif dans le champ **Application Name** (nom de l'application).
6. Pour chaque entrée, entrez le même numéro de port dans les champs **External Port** (port externe) et **Internal Port** (port interne).
7. Dans le champ **To IP Address** (vers adresse IP), entrez les trois derniers chiffres de l'adresse IP réservée pour l'ordinateur vers lequel vous voulez rediriger le trafic Internet. Le reste de l'adresse IP est déjà rempli.
8. Sélectionnez **Enabled** (activé) à côté du champ *IP Address* (adresse IP).



9. Cliquez sur **Save Changes** (enregistrer les modifications) au bas de l'écran.

REMARQUE

Si vous souhaitez utiliser un logiciel tel que VNC sur plusieurs ordinateurs, vous devrez reconfigurer les ports que VNC utilise par défaut sur chaque ordinateur supplémentaire. Ensuite, créez de nouvelles entrées de routage de port pour chaque ordinateur supplémentaire. Reportez-vous à la documentation du logiciel pour obtenir de l'aide.

Configuration du routage d'une plage de ports

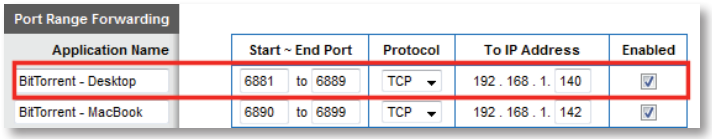
Dans quels cas utiliser le routage d'une plage de ports? Le routage de ports redirige le trafic entrant d'Internet depuis une plage de ports vers un seul périphérique de votre réseau local. Contrairement à une caméra Web qui nécessite généralement le routage d'un port unique, certaines applications requièrent le routage d'une plage de ports.

Exemple : Vous avez besoin de configurer votre ordinateur afin d'utiliser BitTorrent, une application de partage de fichiers poste à poste courante. Par défaut, BitTorrent utilise le port 6881. Si ce port est occupé, le client BitTorrent à l'origine de la requête tente d'utiliser le prochain port de la séquence. En général, dans le cas de routeurs de réseaux domestiques associés à un seul ordinateur BitTorrent, la plage de ports est comprise entre 6881 et 6889.

Pour configurer le routage d'une plage de ports :

Applications & Gaming (applications et jeux) > Port Range Forwarding (routage d'une plage de ports)

1. Accédez à l'utilitaire Web (reportez-vous à la section « Ouverture de l'utilitaire Web », page 18).
2. Configurez la réservation DHCP pour l'adresse IP de l'ordinateur sur lequel vous avez installé le logiciel. (Reportez-vous à la section « Configuration du serveur DHCP sur votre routeur », page 20). Dans cet exemple, l'adresse IP de l'ordinateur sur lequel est installé BitTorrent est 192.168.1.140.
3. Cliquez sur l'onglet **Applications & Gaming** (applications et jeux), puis sur la page **Port Range Forwarding** (routage d'une plage de ports).
4. Entrez un nom descriptif, puis précisez la plage en entrant des valeurs dans les champs **Start Port** (port de départ) et **End Port** (port de fin). Dans cet exemple, la plage s'étend de 6881 à 6889.
5. Sélectionnez le protocole **TCP**.
6. Dans le champ **To IP Address** (vers adresse IP), entrez les trois derniers chiffres de l'adresse IP du périphérique qui exécute le logiciel. Le reste des champs d'adresse IP est déjà rempli. Dans cet exemple, la valeur à entrer est 140.
7. Sélectionnez **Enabled** (activé) à côté du champ *To IP Address* (vers adresse IP).



8. Cliquez sur **Save Settings** (enregistrer les paramètres) au bas de la page.

REMARQUES :

Pour utiliser un logiciel tel que BitTorrent sur plusieurs ordinateurs de votre réseau, créez des entrées supplémentaires à l'aide d'une plage de ports unique, tel qu'indiqué précédemment. BitTorrent ne fonctionne qu'avec les ports compris entre 6881 et 6999.

Selon le pare-feu dont est équipé votre ordinateur, vous devrez ouvrir une plage de ports au sein du pare-feu afin que le logiciel puisse utiliser le routage de plage de ports.

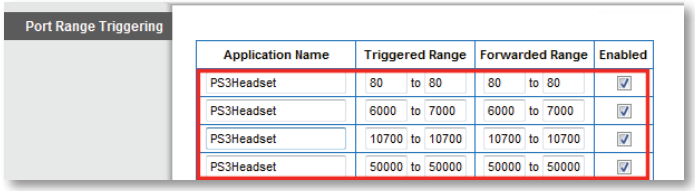
Configuration du déclenchement d'une plage de ports pour le jeu en ligne

Dans quels cas utiliser le déclenchement plutôt que le routage de port? Le déclenchement de plage de ports permet d'indiquer au routeur de surveiller le trafic sortant sur des numéros de port spécifiques. L'adresse IP de l'ordinateur qui transmet les données correspondantes est mémorisée par le routeur, de sorte que lorsque les données demandées sont reçues par celui-ci, elles sont acheminées à l'ordinateur approprié. Le déclenchement de plage de ports intervient par exemple lorsqu'il est nécessaire d'activer un casque USB ou Bluetooth pour le jeu et la discussion en ligne.

Pour configurer le déclenchement d'une plage de ports pour plusieurs entrées :

Applications & Gaming (applications et jeux) > Port Range Triggering (déclenchement de plage de ports)

1. Accédez à l'utilitaire Web (reportez-vous à la section « Ouverture de l'utilitaire Web », page 18).
2. Cliquez sur l'onglet **Applications & Gaming** (applications et jeux), puis sur la page **Port Range Triggering** (déclenchement de plage de ports).
3. Consultez la documentation de votre périphérique pour en savoir plus sur les ports qu'il utilise.
4. Pour chaque entrée de la table *Port Range Forwarding* (routage d'une plage de ports) :
   - Entrez un nom descriptif (par exemple *Casque PS3*).
   - Pour les ports uniques, entrez le même numéro de port dans chaque champ **Triggered Range** (ports déclenchés) et **Forwarded Range** (ports redirigés).
   - Pour les plages de ports, entrez la même plage dans chaque champ **Triggered Range** (ports déclenchés) et **Forwarded Range** (ports redirigés).



5. Cliquez sur **Save Settings** (enregistrer les paramètres) au bas de la page.

Configuration de votre Xbox pour le jeu en ligne

Pourquoi configurer ma Xbox pour le jeu en ligne? Le jeu en ligne ajoute une nouvelle dimension aux parties sur Xbox. Pour bénéficier de cette fonction sur votre Xbox, vous devez rediriger plusieurs ports (comme pour les autres consoles de jeu et applications de jeu en ligne). La procédure de configuration de votre Xbox est presque identique à celle de la configuration du routage de plusieurs ports pour l'accès à distance par VNC. (Reportez-vous à la section « Configuration du routage pour plusieurs ports », page 47).

REMARQUE
Pour en savoir plus sur la configuration du routeur pour le jeu en ligne, reportez-vous à la section « Optimisation de votre routeur pour les jeux et les communications vocales », page 23.

Reportez-vous à la documentation de votre console pour savoir quels ports elle utilise. La Xbox utilise quatre ports :

- Port TCP 80
- Port UDP 88
- Port TCP/UDP 53
- Port TCP/UDP 3074

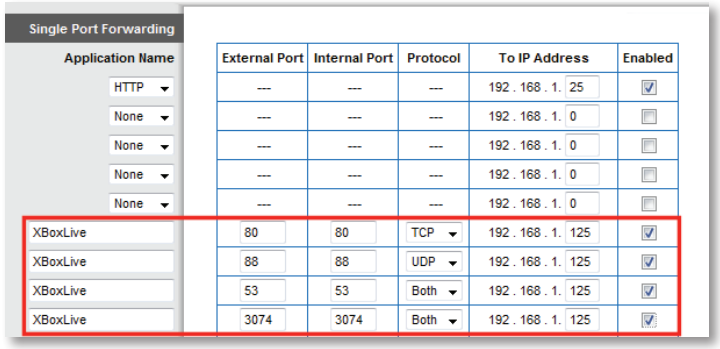
Pour configurer une Xbox à l'aide de plusieurs entrées de routage de port unique :

Applications & Gaming (applications et jeux) > Single Port Forwarding (routage de port unique)

1. Connectez votre Xbox 360 à votre routeur.
2. Accédez à l'utilitaire Web (reportez-vous à la section « Ouverture de l'utilitaire Web », page 18).
3. Configurez une réservation DHCP pour l'adresse IP de la Xbox. (Reportez-vous à la section « Configuration du serveur DHCP sur votre routeur », page 20.).

   – OU –

   Reportez-vous à la documentation de votre console afin de savoir comment définir une adresse IP statique pour votre périphérique.
4. Cliquez sur l'onglet **Applications & Gaming** (applications et jeux), puis sur la page **Single Port Forwarding** (routage de port unique). La Xbox utilise quatre ports. Vous devez donc créer quatre entrées de routage de port sur cette page.
5. Entrez les données relatives au port et au protocole, comme indiqué ci-dessous.


Single Port Forwarding
Application Name
External Port
Internal Port
Protocol
To IP Address
Enabled
HTTP --- --- --- 192 . 168 . 1. 25
None --- --- --- 192 . 168 . 1. 0
None --- --- --- 192 . 168 . 1. 0
None --- --- --- 192 . 168 . 1. 0
None --- --- --- 192 . 168 . 1. 0
XBoxLive 80 80 TCP 192 . 168 . 1. 125
XBoxLive 88 88 UDP 192 . 168 . 1. 125
XBoxLive 53 53 Both 192 . 168 . 1. 125
XBoxLive 3074 3074 Both 192 . 168 . 1. 125

6. Dans le champ **To IP Address** (vers adresse IP), entrez un numéro de 1 à 3 chiffres correspondant aux trois derniers chiffres de l'adresse IP de la Xbox 360. Le reste de l'adresse IP est déjà rempli.
7. Sélectionnez **Enabled** (activé) à côté du champ *To IP Address* (vers adresse IP) pour chaque entrée.
8. Cliquez sur **Save Settings** (enregistrer les paramètres) au bas de la page.

Mise à jour et surveillance

Sauvegarde et rétablissement de la configuration de votre routeur

Pourquoi sauvegarder la configuration de mon routeur? Comme c'est le cas pour toutes les données importantes, il est essentiel de sauvegarder la configuration de votre routeur. Votre routeur peut contenir de nombreux paramètres personnalisés. Si vous le réinitialisez et que vous rétablissez les valeurs par défaut, vous perdrez les paramètres personnalisés et vous devrez de nouveau les entrer manuellement. En sauvegardant la configuration, vous pourrez facilement rétablir les paramètres de votre routeur.

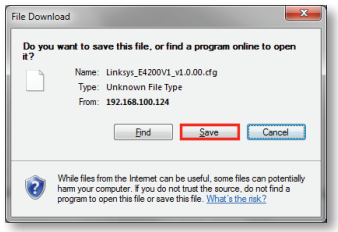
Pour sauvegarder la configuration de votre routeur :

Administration > Management (gestion)

1. Accédez à l'utilitaire Web (reportez-vous à la section « Ouverture de l'utilitaire Web », page 18).
2. Cliquez sur l'onglet **Administration** puis sur la page **Management** (gestion).
3. Cliquez sur **Back Up Configurations** (sauvegarder les configurations) au bas de l'écran.

Un message vous invite à enregistrer le fichier.

4. Cliquez sur **OK** ou **Save** (enregistrer).

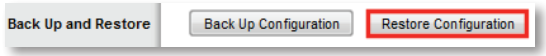

File Download
Do you want to save this file, or find a program online to open it?
Name: Linksys_E4200V1_v1.0.00.cfg
Type: Unknown File Type
From: 192.168.100.124
Find
Save
Cancel
While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not find a program to open this file or save this file. What's the risk?

5. Choisissez l'emplacement du fichier, puis cliquez sur **Save** (enregistrer).

Pour rétablir la configuration de votre routeur :

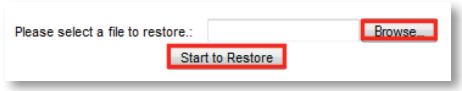
Administration > Management (gestion)

1. Accédez à l'utilitaire Web (reportez-vous à la section « Ouverture de l'utilitaire Web », page 18).
2. Cliquez sur l'onglet **Administration** puis sur la page **Management** (gestion).
3. Cliquez sur **Restore Configurations** (rétablir les configurations) au bas de l'écran.



Une nouvelle fenêtre s'affiche.

4. Cliquez sur **Browse** (parcourir) pour accéder à l'emplacement du fichier de configuration, sélectionnez ce dernier et cliquez sur **Open** (ouvrir).
5. Pour rétablir la configuration, cliquez sur **Start to Restore** (commencer la restauration).



Rétablissement des valeurs par défaut

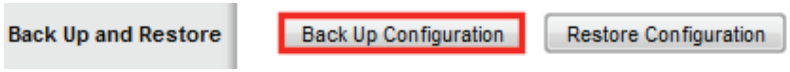
Dans quels cas rétablir les valeurs par défaut? Si vous ne parvenez pas à résoudre certains problèmes après avoir suivi toutes les procédures de dépannage, vous devrez peut-être rétablir les valeurs par défaut du routeur. La réinitialisation efface tous vos paramètres. Vous devrez donc les rétablir ultérieurement. Nous vous conseillons de sauvegarder votre configuration avant de rétablir les valeurs par défaut du routeur. Reportez-vous à la section « Sauvegarde et rétablissement de la configuration de votre routeur », page 50.

Pour rétablir les valeurs par défaut, appuyez sur le bouton de réinitialisation du routeur ou utilisez l'utilitaire Web.

Pour réinitialiser les valeurs par défaut à l'aide du bouton de réinitialisation :

1. Assurez-vous que le routeur est sous tension et allumé. Maintenez le bouton **Reset** (réinitialiser) du routeur enfoncé entre 5 et 10 secondes.

Bouton de réinitialisation des modèles E1200, E1500, E2500 et E3200

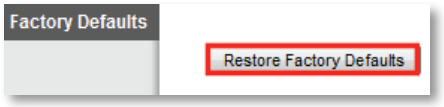


Bouton de réinitialisation du modèle E4200

Pour réinitialiser les valeurs par défaut à l'aide de l'utilitaire Web :

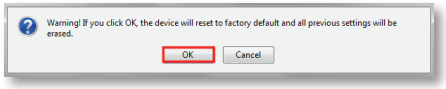
Administration > Factory Defaults (valeurs par défaut)

1. Accédez à l'utilitaire Web (reportez-vous à la section « Ouverture de l'utilitaire Web », page 18).
2. Cliquez sur l'onglet **Administration** puis sur la page **Factory Defaults** (valeurs par défaut).
3. Cliquez sur **Restore Factory Defaults** (rétablir les valeurs par défaut).



Une fenêtre de confirmation s'affiche.

4. Cliquez sur **OK**.



Mise à niveau du microcode de votre routeur

Dans quel cas est-il nécessaire de mettre à niveau le microcode de mon routeur? Linksys publie régulièrement des mises à jour du microcode pour corriger un problème ou ajouter des fonctionnalités à votre routeur.

IMPORTANT

N'interrompez pas la procédure de mise à niveau. N'éteignez pas le routeur et n'appuyez pas sur le bouton de réinitialisation pendant la mise à niveau. Vous risqueriez de désactiver définitivement le routeur.

Si vous procédez à la mise à niveau depuis un ordinateur portatif, assurez-vous que ce dernier est relié à une source d'alimentation ou que la batterie est complètement chargée.

Désactivez le mode de mise en veille de votre ordinateur. La veille risquerait d'interrompre la procédure de mise à niveau.

Si vous devez effectuer une mise à niveau depuis un ordinateur doté d'une connexion réseau sans fil, assurez-vous que le signal est suffisamment puissant. Si ce n'est pas le cas, rapprochez l'ordinateur du routeur.

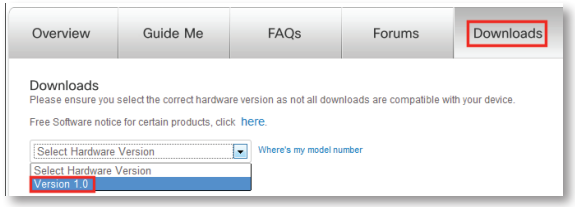
CONSEILS

Cisco Connect recherche et installe systématiquement les mises à jour. Suivez les instructions ci-après uniquement si vous n'utilisez pas Cisco Connect.

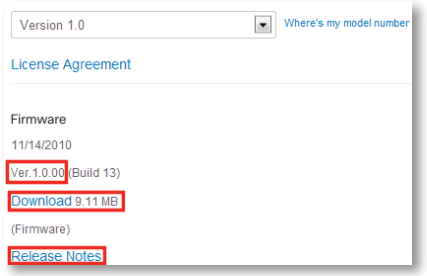
Pour mettre à niveau le microcode de votre routeur :

Linksys.com/support
Administration > Firmware Upgrade (mise à niveau du microcode)

1. Accédez à l'utilitaire Web (reportez-vous à la section « Ouverture de l'utilitaire Web », page 18).
2. Cliquez sur l'onglet **Status** (état), puis sur la page **Router** (routeur). Notez la version actuelle du microcode de votre routeur.
3. Ouvrez un navigateur Web, connectez-vous à la page **Linksys.com/support**, puis recherchez le modèle de votre routeur.
4. Cliquez sur l'onglet **Downloads** (téléchargements), sélectionnez la version matérielle de votre routeur dans la liste déroulante **Select Hardware Version** (sélectionner la version matérielle).

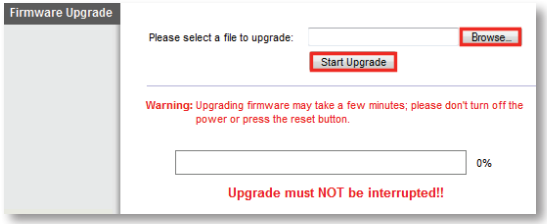


5. Comparez la dernière version du microcode disponible sur le site Web avec votre version actuelle. Si une nouvelle version est disponible, cliquez sur **Release Notes** (notes de version) afin de déterminer si cette version plus récente contient de nouvelles fonctionnalités ou permet de corriger un problème.
6. Si vous le souhaitez, cliquez sur **Download** (télécharger) et enregistrez le fichier sur votre ordinateur. Notez l'emplacement du fichier.



Durant la procédure de mise à niveau, le routeur risque d'effacer les paramètres que vous avez modifiés. Sauvegardez la configuration de votre routeur *avant* la mise à niveau. Reportez-vous à la section « Sauvegarde et rétablissement de la configuration de votre routeur », page 50.

7. Dans l'utilitaire Web, cliquez sur l'onglet **Administration**, puis sur la page **Firmware Upgrade** (mise à niveau du microcode).
8. Cliquez sur **Browse** (parcourir) puis accédez à l'emplacement où vous avez enregistré le fichier.
9. Sélectionnez le fichier de mise à niveau, cliquez sur **Start Upgrade** (lancer la mise à niveau) et suivez les instructions à l'écran. La procédure de mise à niveau commence et une barre de progression s'affiche. Une fois le microcode chargé, une page s'ouvre pour vous aviser que la mise à niveau a réussi (Upgrade is successful), puis le routeur redémarre.


Firmware Upgrade
Please select a file to upgrade:
Browse...
Start Upgrade
Warning: Upgrading firmware may take a few minutes; please don't turn off the power or press the reset button.
0%
Upgrade must NOT be interrupted!!

Vérification de l'état de votre routeur

Pourquoi vérifier l'état de mon routeur? L'état de votre routeur indique votre connexion Internet est sécurisée et donne des renseignements sur l'état des périphériques connectés au réseau.

Pour vérifier l'état de votre routeur à l'aide de Cisco Connect :

1. Sous Windows, cliquez sur **Démarrer**, **Programmes**, puis sur **Cisco Connect**.

   – OU –

   Sous Mac, ouvrez le dossier **Applications** et cliquez sur **Cisco Connect**.

   Le menu principal de Cisco Connect s'ouvre.

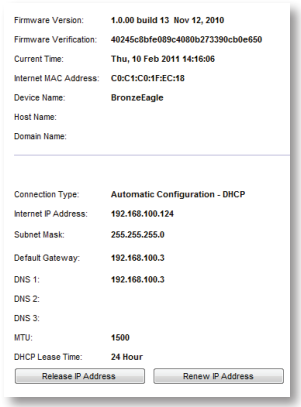
2. Regardez dans le coin supérieur droit du menu principal Cisco Connect. Si votre routeur est en ligne et sécurisé, la mention *online secure* (en ligne et sécurisé) apparaît, accompagnée d'un point vert.

Pour vérifier l'état de votre routeur à l'aide de l'utilitaire Web :

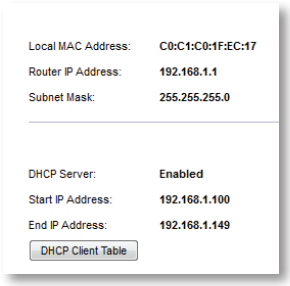
Status (état) > Router (routeur)
Status (état) > Local Network (réseau local)
Status (état) > Wireless Network (réseau sans fil)
Status (état) > Ports

1. Accédez à l'utilitaire Web (reportez-vous à la section « Ouverture de l'utilitaire Web », page 18).
2. Cliquez sur l'onglet **Status** (état) puis sur la page **Router** (routeur). La page affiche de l'information détaillée sur l'état de votre routeur.

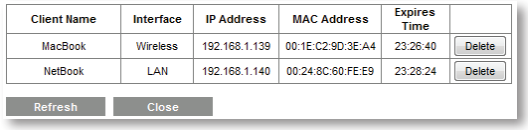
CONSEIL
Pour voir la description des champs, cliquez sur **Help** (aide) à droite de l'écran.



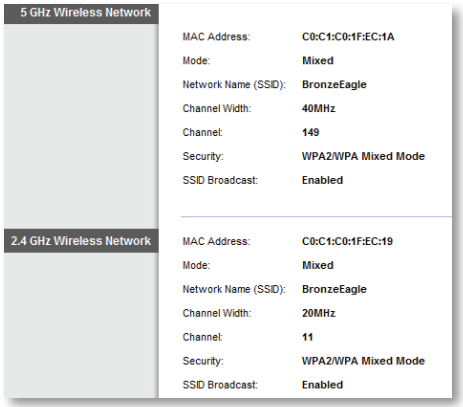
3. Cliquez sur l'onglet **Status** (état) puis sur la page **Local Network** (réseau local). La page affiche de l'information sur l'adresse IP de votre réseau local et les paramètres de serveur DHCP.



4. Cliquez sur **DHCP Client Table** (table des clients DHCP) pour voir l'adresse IP actuellement attribuée.



5. Cliquez sur l'onglet **Status** (état) puis sur la page **Wireless Network** (réseau sans fil). L'état de votre réseau sans fil s'affiche.



6. Cliquez sur l'onglet **Status** (état) puis sur la page **Ports**. La page affiche l'état et la vitesse de la connexion pour chaque port Ethernet et pour le port Internet (données de vitesse uniquement disponibles sur les modèles E3200 et E4200).

Désactivation des voyants d'état des ports Ethernet

Pourquoi désactiver les voyants d'état des ports Ethernet? Selon l'endroit où est placé votre routeur, les voyants peuvent s'avérer gênants. Pour les désactiver, utilisez Cisco Connect ou l'utilitaire Web.

Pour désactiver les voyants à l'aide de Cisco Connect :

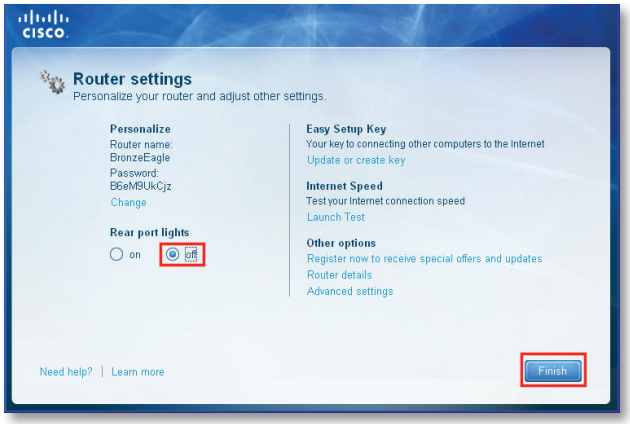
1. Sous Windows, cliquez sur **Démarrer**, **Programmes**, puis sur **Cisco Connect**.

   – OU –

   Sous Mac, ouvrez le dossier **Applications** et cliquez sur **Cisco Connect**.

   Le menu principal de Cisco Connect s'ouvre.

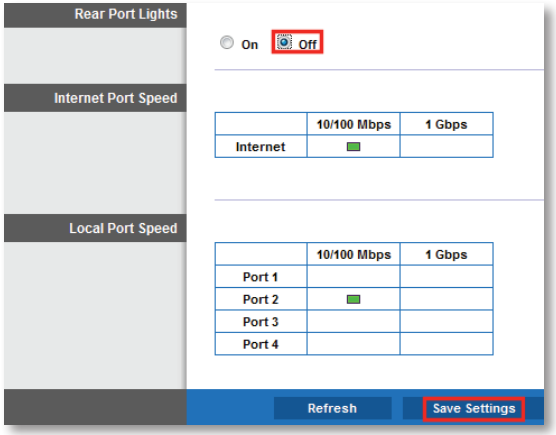
2. Sous *Router Settings* (paramètres du routeur), cliquez sur **Change** (modifier).
3. Sous *Port lights* (voyants des ports), cliquez sur **Off** (désactivé) puis sur **Finish** (terminé).



Pour désactiver les voyants à l'aide de l'utilitaire Web :

Status (état) > Ports

1. Accédez à l'utilitaire Web (reportez-vous à la section « Ouverture de l'utilitaire Web », page 18).
2. Cliquez sur l'onglet **Status** (état) puis sur la page **Ports**.
3. Dans la section *Rear Port Lights* (voyants du port arrière), cliquez sur **Off** (désactivé), puis sur **Save Settings** (enregistrer les paramètres).



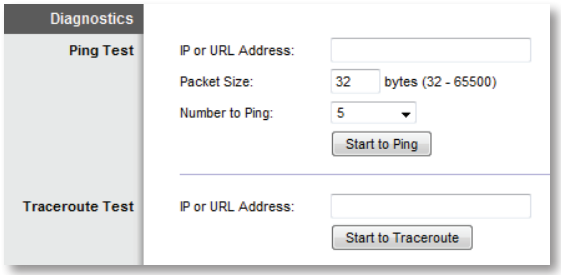
Test de votre connexion Internet

Quels utilitaires mon routeur intègre-t-il pour tester la connexion Internet? Votre routeur intègre deux tests de diagnostic : Ping et Traceroute. Ils permettent de vérifier vos connexions réseau, notamment la connexion Internet et celle des périphériques réseau.

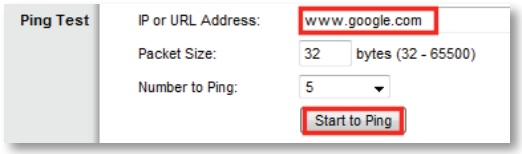
Pour diagnostiquer votre connexion Internet :

Administration > Diagnostics

1. Accédez à l'utilitaire Web (reportez-vous à la section « Ouverture de l'utilitaire Web », page 18).
2. Cliquez sur l'onglet **Administration** puis sur la page **Diagnostics**.



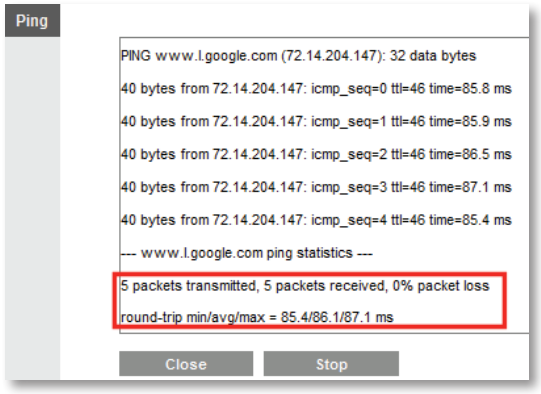
3. Pour savoir s'il est possible d'atteindre une adresse, entrez une adresse IP ou une URL, une taille de paquet et le nombre de ping dans la section *Ping Test* (test ping), puis cliquez sur **Start to Ping** (démarrer le test ping).



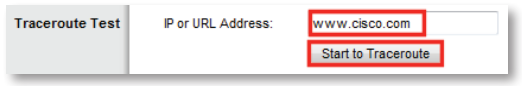
Une fenêtre s'ouvre pour afficher les résultats du test ping. Une réponse apparaît pour chaque test ping réussi.

REMARQUE

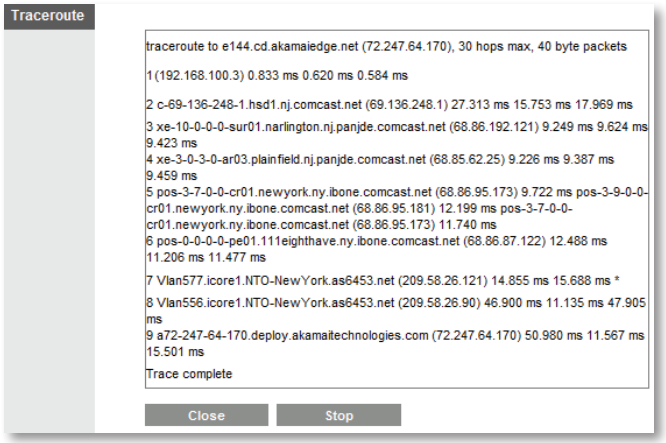
Si une URL Internet ne répond pas au test ping, cela ne signifie pas nécessairement que le site est indisponible. Pour des raisons de sécurité, certains sites sont configurés de sorte à ne pas répondre aux requêtes ping.


Ping
PING www.l.google.com (72.14.204.147): 32 data bytes
40 bytes from 72.14.204.147: icmp_seq=0 ttl=46 time=85.8 ms
40 bytes from 72.14.204.147: icmp_seq=1 ttl=46 time=85.9 ms
40 bytes from 72.14.204.147: icmp_seq=2 ttl=46 time=86.5 ms
40 bytes from 72.14.204.147: icmp_seq=3 ttl=46 time=87.1 ms
40 bytes from 72.14.204.147: icmp_seq=4 ttl=46 time=85.4 ms
--- www.l.google.com ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 85.4/86.1/87.1 ms
Close
Stop

4. Pour suivre l'acheminement des paquets entre votre routeur et une adresse spécifique, entrez une adresse dans le champ **IP** (adresse IP) ou **URL Address** (adresse URL) de la zone *Traceroute Test* (test Traceroute), puis cliquez sur **Start to Traceroute** (démarrer le test Traceroute).



Une fenêtre s'ouvre pour afficher les résultats du test.


Traceroute
traceroute to e144.cd.akamaiedge.net (72.247.64.170), 30 hops max, 40 byte packets
1 (192.168.100.3) 0.833 ms 0.620 ms 0.584 ms
2 c-69-136-248-1.hsd1.nj.comcast.net (69.136.248.1) 27.313 ms 15.753 ms 17.969 ms
3 xe-10-0-0-0-sur01.narlington.nj.panjde.comcast.net (68.86.192.121) 9.249 ms 9.624 ms 9.423 ms
4 xe-3-0-3-0-ar03.plainfield.nj.panjde.comcast.net (68.85.62.25) 9.226 ms 9.387 ms 9.459 ms
5 pos-3-7-0-0-cr01.newyork.ny.ibone.comcast.net (68.86.95.173) 9.722 ms pos-3-9-0-0-cr01.newyork.ny.ibone.comcast.net (68.86.95.181) 12.199 ms pos-3-7-0-0-cr01.newyork.ny.ibone.comcast.net (68.86.95.173) 11.740 ms
6 pos-0-0-0-0-pe01.111eighthave.ny.ibone.comcast.net (68.86.87.122) 12.488 ms 11.206 ms 11.477 ms
7 Vlan577.icore1.NTO-NewYork.as6453.net (209.58.26.121) 14.855 ms 15.688 ms *
8 Vlan556.icore1.NTO-NewYork.as6453.net (209.58.26.90) 46.900 ms 11.135 ms 47.905 ms
9 a72-247-64-170.deploy.akamaitechnologies.com (72.247.64.170) 50.980 ms 11.567 ms 15.501 ms
Trace complete
Close
Stop

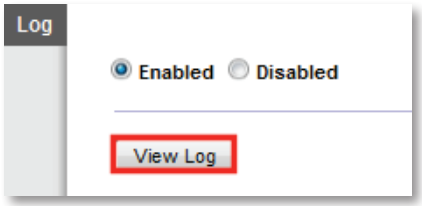
Configuration et utilisation des journaux

De quels types de journaux est doté mon routeur? Votre routeur effectue le suivi du trafic pour toutes vos connexions à Internet. Votre routeur prend en charge quatre types de journaux :

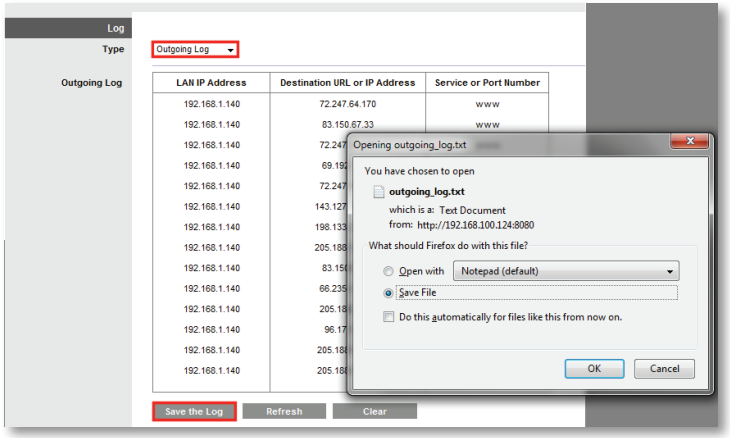
Pour activer et consulter les journaux de votre routeur :

Administration > Log (journal)

1. Accédez à l'utilitaire Web (reportez-vous à la section « Ouverture de l'utilitaire Web », page 18).
2. Cliquez sur l'onglet **Administration** puis sur la page **Log** (journal).
3. Pour surveiller le trafic entre le réseau local et Internet, conservez l'option par défaut **Enabled** (activé), puis cliquez sur **Save Settings** (enregistrer les paramètres).
4. Pour consulter les journaux, cliquez sur **View Log** (afficher le journal). La fenêtre *Log* (journal) s'ouvre.



5. Sélectionnez le journal que vous voulez consulter dans la liste déroulante **Type**.



- **Incoming Log** (journal des entrées) : Affiche les adresses IP sources et les numéros de port de destination du trafic Internet entrant
- **Outgoing Log** (journal sortant) : Affiche les adresses IP locales, les URL/adresses IP de destination et les numéros de port/service du trafic Internet sortant
- **Security Log** (journal de sécurité) : Données de connexion à l'utilitaire Web
- **DHCP Client Log** (journal des activités des clients DHCP) : Information sur l'état du serveur DHCP local

6. Pour enregistrer le journal, cliquez sur **Save the Log** (enregistrer le journal) puis cliquez sur **OK** ou **Save** (enregistrer).

Structure des menus de l'utilitaire Web

Linksys E1550

Setup (configuration)
- Basic Setup (configuration de base)
  - Language (langue)
  - Internet Setup (configuration Internet)
    - Internet Connection Type (type de connexion Internet)
    - Optional Settings (paramètres facultatifs)
  - Network Setup (configuration du réseau)
    - Router Address (adresse du routeur)
    - DHCP Server Setting (paramètres de serveur DHCP)
  - Time Settings (fuseau horaire)
    - Time Zone (fuseau horaire)
  - Reboot (redémarrage)
- IPv6 Setup (configuration IPv6)
  - Internet Setup (configuration Internet)
    - Internet Connection Type (type de connexion Internet)
  - Network Setup (configuration du réseau)
    - 6rd Tunnel (Tunnel 6rd)
- DDNS
  - DDNS Service (service DDNS)
- MAC Address Clone (clonage d'adresse MAC)
- Advanced Routing (routage avancé)
  - NAT (traduction des adresses réseau)
  - Dynamic Routing (RIP) (routage dynamique RIP)
  - Static Routing (routage statique)

Wireless (sans fil)
- Basic Wireless Settings (paramètres de base du réseau sans fil)
  - Wi-Fi Protected Setup (configuration de l'accès Wi-Fi protégé)
    - 5 GHz Wireless Settings (paramètres sans fil 5 GHz)
    - 2.4 GHz Wireless Settings (paramètres sans fil 2,4 GHz)
    - Configuration View (vue de configuration)
- Wireless Security (sécurité sans fil)
  - 5 GHz Wireless Security (sécurité sans fil 5 GHz)
  - 2.4 GHz Wireless Security (sécurité sans fil 2,4 GHz)
- Guest Access (accès d'invité)
- Wireless MAC Filter (filtrage des adresses MAC sans fil)
  - Wireless MAC Filter (filtrage des adresses MAC sans fil)
    - Access Restriction (restriction d'accès)
    - MAC Address Filter List (liste de filtrage d'adresses MAC)

Security (sécurité)
- Firewall (pare-feu)
  - Firewall (pare-feu)
  - Internet Filter (filtre Internet)
  - Web Filter (filtre Web)
- VPN Passthrough (intercommunication VPN)

Storage (stockage)
- Disk (disque)
  - Disk Management (gestion des disques)
    - Shared Folder (dossier partagé)
    - Format Disk (formater le disque)
- FTP Server (serveur FTP)
  - Setup (configuration)
  - Access (accès)
- Administration
  - Information
  - Anonymous Access (accès anonyme)
  - User Management (gestion des utilisateurs)
  - Group Management (gestion des groupes)

Access Policy (politique d'accès)
- Parental Controls (contrôle parental)
  - Target Devices (périphériques cibles)
  - Schedule (planification)
  - Block Specific Sites (blocage de sites spécifiques)

Applications & Gaming (applications et jeux)
- Single Port Forwarding (routage de port unique)
  - Application Name (nom de l'application)
- Port Range Forwarding (routage d'une plage de ports)
  - Application Name (nom de l'application)
- Port Range Triggering (déclenchement de plage de ports)
- DMZ (zone publique)
- QoS (qualité du service)
  - QoS (qualité du service)
    - Wireless (sans fil)
    - Internet Access Priority (priorité d'accès Internet)
    - Upstream Bandwidth (bande passante montante)
    - Category (catégorie)
    - Summary (sommaire)

Administration
- Management (gestion)
  - Router Access (accès au routeur)
  - Local Management Access (accès de gestion local)
  - Remote Management Access (accès de gestion à distance)
  - Advanced features (fonctionnalités avancées)
  - UPnP
  - Back up and Restore (sauvegarde et restauration)
- Log (journal)
- Diagnostics
  - Ping Test (test Ping)
  - Traceroute Test (test Traceroute)

- Factory Defaults (valeurs par défaut)
- Firmware Upgrade (mise à niveau du microcode)

Status (état)

- Router (routeur)
  - Router Information (renseignements sur le routeur)
  - Internet Connection (connexion Internet)
    - IPv4
    - IPv6
- Local Network (réseau local)
  - Local Network (réseau local)
  - DHCP Server (serveur DHCP)
- Wireless Network (réseau sans fil)
  - 5 GHz Wireless Network (réseau sans fil 5 GHz)
  - 2.4 GHz Wireless Network (réseau sans fil 2,4 GHz)
- Ports
  - Rear Port Lights (voyants de port arrière)
  - Internet Port Link (connexion du port Internet)
  - Local Port Link (connexion du port local)

Caractéristiques techniques

Linksys E1550

Nom du modèle	Linksys E1550
Description	Routeur sans fil N avec SpeedBoost
Numéro de modèle	E1500
Normes	802.11n, 802.11g, 802.11b, 802.3u
Ports	Alimentation, Internet, Ethernet (1 à 4), USB
Boutons	Réinitialisation, Wi-Fi Protected Setup
Voyants	Alimentation/Wi-Fi Protected Setup, Internet, Ethernet (1 à 4)
Câblage	Catégorie 5e
Puissance de transmission	802.11b: 16.5 ± 1.5 dBm 802.11g: 14.5 ± 1.5 dBm 802.11n : (20 MHz): 15.0 ± 1.5 dBm sur canal 6, MCS0, 8 (20 MHz): 13.5 ± 1.5 dBm sur canal 6, MCS7, 15 (40 MHz): 13.5 ± 1.5 dBm sur canal 6, MCS0, 7, 8,
Gain d'antenne	Antenna 1: ≤ 2.5 dBi Antenna 2: ≤ 3 dBi Antenna 3 ≤ 4 dBi
Sensibilité en réception	802.11b: -87 dBm à 11 Mbps (Type) 802.11g: -71 dBm à 54 Mbps (Type) 802.11n (20 MHz): -69 dBm à MCS15 (Type) 802.11n (40 MHz): -66 dBm à MCS15 (Type)
UPnP	Pris en charge
Sécurité sans fil	WPA2 (Wi-Fi Protected Access™ 2), WPA, WEP
Bits de clé de sécurité	Cryptage de données jusqu'à 128 bits

Environnement d'exploitation

Dimensions	7,95 × 6,3 × 1,34 po (202 × 160 × 34 mm)
Poids	280 g (9,81 oz)
Alimentation	12 V, 1,5 A
Homologations	FCC, UL/cUL, ICES-003, CE, Wi-Fi (IEEE 802.11b/g/n), Windows 7
Température (fonctionnement)	32 à 104°F (0 à 40°C)
Température (entreposage)	-4 à 140°F (-20 à 60°C)
Humidité (fonctionnement)	10 à 80 %, sans condensation
Humidité (entreposage)	5 à 90 %, sans condensation

Les spécifications peuvent changer sans préavis.

Visitez la page **linksys.com/support** pour bénéficier de nos services de soutien techniques primés 24 heures sur 24 et 7 jours sur 7.

Cisco, le logo Cisco, Flip et Linksys sont des marques de commerce ou des marques déposées de Cisco ou de ses sociétés affiliées aux États-Unis et dans d'autres pays.
Vous trouverez une liste des marques de commerce de Cisco à l'adresse www.cisco.com/go/trademarks. Les autres marques de commerce mentionnées dans ce document sont la propriété de leurs détenteurs respectifs.

© Cisco ou ses sociétés affiliées, 2011. Tous droits réservés.

3425-00977